MODELING INFORMATION ASSURANCE:

A VALUE FOCUSED THINKING APPROACH

THESIS

Jonathan Todd Hamill, Captain, USAF

AFIT/GOR/ENS/00M-15

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

20000815 193

The views expressed in this thesis are those of the author and do not reflect the official policy or

position of the United States Air Force, Department of Defense, or the U. S. Government.

MODELING INFORMATION ASSURANCE:

A VALUE FOCUSED THINKING APPROACH

THESIS

Presented to the Faculty

Department of Operational Sciences

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Science in Operations Research

Jonathan T. Hamill, M.S.

Captain, USAF

March 2000

MODELING INFORMATION ASSURANCE:

A VALUE FOCUSED THINKING APPROACH

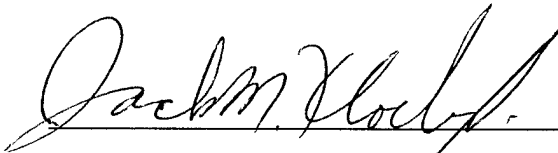Jonathan T. Hamill, M.S.

Captain, USAF

Approved:

_____

Richard F. Deckro, DBA (Advisor)
Professor of Operations Research
Department of Operational Sciences

14 March 2000

date

_____

Jack M. Kloeber Jr., PhD, Lieutenant Colonel, USA
Associate Professor of Operations Research
Department of Operational Sciences

14 March 2000

date

ACKNOWLEDGEMENTS

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF EQUATIONS

ABSTRACT

The information revolution has brought forth new and improved capabilities to rapidly disseminate and employ information in decision-making. These capabilities are critical to the civilian and military infrastructures of the United States, and act as force enhancers and enablers for the Armed Forces. These capabilities, however, often rely upon systems interconnected throughout the world, resulting in potentially increased vulnerability to attack. To add to this problem, elusive, threatening forces (national and transnational) originating from anywhere on the globe are likely to offer opponents less reliant on information technology an asymmetric advantage over information-reliant nations like the United States.

To date, effective methods and measures to specifically value information and information systems are lacking. This thesis develops a first cut methodology facilitating the identification of key information, generating information assurance strategies and implementing measures to assess them.

MODELING INFORMATION ASSURANCE:

A VALUE FOCUSED THINKING APPROACH

1. Introduction

1.1. Background

The tremendous worldwide increase in reliance upon information technologies (IT) reaps huge benefits for their users but also threatens significant drawbacks. These technologies afford decision-makers with the capability to quickly fuse data from multiple sources, make informed decisions, and disseminate those decisions to necessary units and personnel at nearly the speed of light. Such IT capabilities have become necessary for day-to-day operations for many agencies (government and civilian), and offer tremendous military advantages over opponents during times of crisis.

Research and development of information technologies began with the Advanced Research Projects Agency Network (ARPANET), which has evolved into today's Internet. However, the "ARPANET protocols (the rules of syntax that enable computers to communicate on a network) were originally designed for openness and flexibility, not for security." [Longstaff, Ellis, Hernan, Lipson, McMillan, Pesante, and Simmel, 1997] The initial approach that permitted "unrestricted insiders" to easily share information is no longer appropriate for today's commercial and government use. [Longstaff, et. al., 1997] Organizations often deal with the subsequent vulnerabilities that develop on an after-the-fact basis, or worse, not at all, leaving the United States' national security exposed to a variety of threats.

Such threats employ widely available tools and easily obtainable technology to seek out and capitalize upon these vulnerabilities. The President's Commission on Critical Infrastructure

Protection (PCCIP) addressed these vulnerabilities on a national scale by identifying five sectors of industry that share common characteristics. In particular, the Commission highlighted the interconnectedness of these key sectors and their heavy reliance upon information technology. The five sectors include

1. Information and Communications
2. Banking and Finance
3. Energy (Including Electrical Power, Oil and Gas)
4. Physical Distribution
5. Vital Human Services [PCCIP, 1997:2]

The information and communications infrastructure (the Internet in particular) has evolved from serving primarily Department of Defense (DOD) and academic institutions to interconnected systems vital to the existence of many of today's organizations. The Internet now effectively spans the entire globe. This expansion resulted from an increased availability and improvements in information technologies, allowing nearly all sectors an opportunity to streamline current operations via more efficient allocation of resources, while simultaneously creating completely new industries. Information systems now monitor and control many of the operations of various other infrastructures. These systems are often an ad hoc mixture of components, processes and software, which were not often designed to inter-operate in a secure fashion. The resulting interdependencies and relatively easy access for a number of threats puts all sectors at risk.

The Persian Gulf War saw an unprecedented use of information technologies in support of combat operations and revealed the "effectiveness and power of Information Age technologies and weaponry." [Gumahad, 1997:15] It also demonstrated that information warfare (IW) attacks on any information-advanced state might devastate its national infrastructure through the destruction or interruption of its financial, communications, electrical or transportation sectors.

[Gumahad, 1997:15] Within the United States, such sectors are interconnected and oftentimes heavily reliant upon similar information technologies.

The lessons offered by the Gulf War, as well as those encountered by numerous "Red Team" exercises (wargame-like activities that seek out and exploit system vulnerabilities in order to evaluate readiness or provide training), have provided military leadership with many new ideas and concerns with regards to information operations (IO). Joint Vision 2010 (JV 2010), for example, foresaw the necessity of Information Superiority, defined as "the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same." [JV 2010, 1996:41] Information Superiority, coupled with advances in technology, provides the foundation of all other aspects of future Joint combat, and allows the possibility of full spectrum dominance. [JV 2010, 1996:46]

Information Operations
Relationships Across the Peace-Conflict Cycle

Peace ———► Crisis ─► Conflict ———► Return to Peace
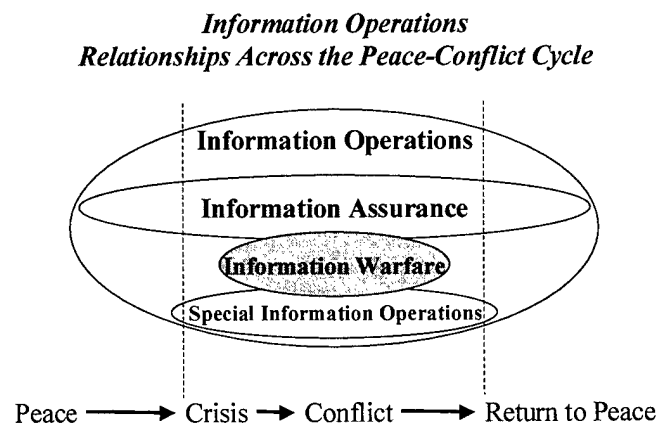
Figure 1-1: IO Relationships [JP 3-13, 1998:I-4]

Figure 1-1 depicts the realms of Information Operations as defined by Joint Doctrine. Joint Publication 3-13 defines IO as "actions taken to affect adversary information and information systems while defending one's own information and information systems." [1998:I-1] This definition alludes to offensive and defensive postures within IO. Joint doctrine cites four interrelated processes as the elements of defensive IO: information environment protection,

attack detection, capability restoration, and attack response. Offensive capabilities can also offer

defense through deterrence of adversary intentions or eliminating their IO capabilities altogether.

Through technology and training, "defensive IO processes integrate all available capabilities to

ensure defense in depth." [JP 3-13, 1998:III-1]

Information Warfare (IW), defined as "IO conducted during time of crisis or conflict

(including war) to achieve or promote specific objectives over a specific adversary or

adversaries," is subsequently a component of IO. [JP 3-13, 1998:I-1] Special information

operations (SIO) are defined as "IO that by their sensitive nature, due to their potential effect or

impact, security requirements, or risk to the national security of the United States, require a

special review and approval process." [JP 1-02, 1999:414] Figure 1-1, which illustrates the IO

relationships across the time spectrum of conflict, shows a third subset of IO that occurs on a

continual basis—Information Assurance.

Joint doctrine offers this definition of information assurance (IA).

> IA protects and defends information and information systems by ensuring
> their availability, integrity, identification and authentication, confidentiality, and
> non-repudiation. This includes providing for the restoration of information
> systems by incorporating protection, detection, and reaction capabilities. IA
> employs technologies and processes such as multilevel security, access controls,
> secure network servers, and intrusion detection software. [JP 3-13, 1998:III-1]

The rationale behind the ceaseless vigilance of IA stems from the growing number of

threats with their increasing capabilities to inflict damage upon information systems. Those

techniques that provided the United States an advantage in the past now pose a threat to not only

our national infrastructure, but to the current and future capabilities of the Armed Forces.

Molander, Wilson, Mussington, and Mesic called such an effort "to hold at risk (not for

destruction, but for large-scale or massive disruption) key national strategic assets such as

elements of various key national infrastructure sectors, such as energy, telecommunications, transportation, and finance)" strategic information warfare (SIW). [Molander, et. al., 1999:1]

To further justify a need for continuous information assurance, these authors also noted that SIW weapons "may find their highest utility in the near-term in asymmetric strategies employed by regional adversaries... that seek to avoid directly challenging U.S. conventional battlefield superiority...." [Molander, et. al., 1999:2] SIW has several advantages offered to potential adversaries. These include:

- The cost of entry is low compared to conventional attack methods.

- Intelligence on 'electronic' threats is difficult to gather.

- Attacks may be difficult to detect, allowing the perpetrator time to either complete the mission prior to discovery, or disengage without being discovered at all, allowing them an increased probability of success with follow-on engagements, due to knowledge gained from system experience.

- Weapon or attack effects may be uncertain, for both the attacker and defender. It is oftentimes difficult to assess the objectives of an attack, which may be vulnerable or continue to be so. [Molander, et. al., 1999:14]

Figure 1-2 illustrates the increasing trend in incidents handled by the Computer Emergency Response Team (CERT). Noting the fact that these incidents are only those that were detected *and* reported implies that a much larger number of attacks have actually occurred. Military exercises like "Eligible Receiver" have demonstrated, with relative ease, hackers' ability to "cripple U.S. military and civilian computer networks...." [Gertz, 1998] These attacks frequently go unreported for either security or financial reasons.
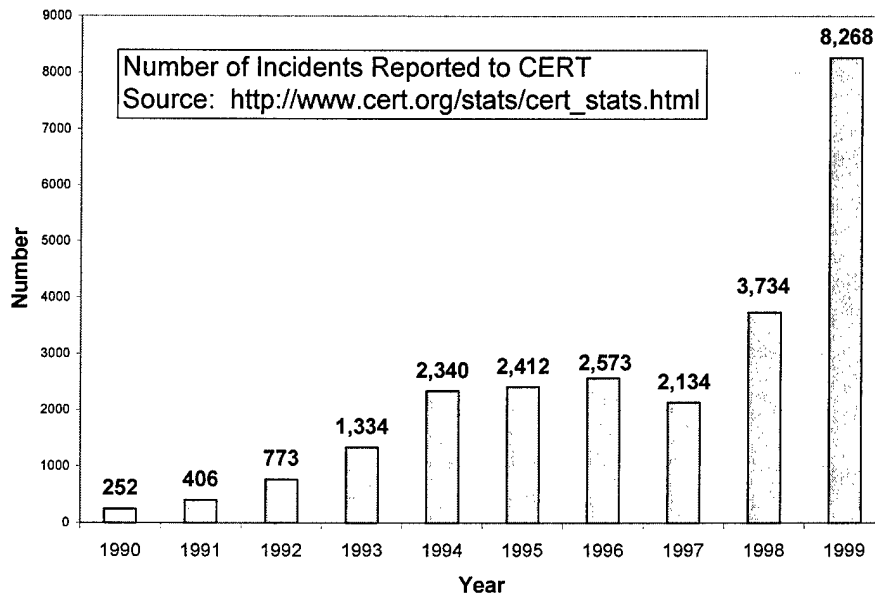
Figure 1-2: Security Incidents [CERT, 2000]

These increasing trends show that IA is a vital strategy for thwarting threats to U.S.

national economic and military security. As time and technology continue to advance,

maintaining normal day-to-day operations and the capability to employ military force at any

given moment will hinge on the continuous development, implementation and improvement of

the level of IA. There has been work detailing the nuances of offensive IO, which provides some

insight into what decision-makers value of their own systems by highlighting the adversary's

systems chosen as targets. [Doyle, 1998; Doyle, et. al., 2000]

1.2. Problem Statement

To provide information assurance, the important aspects of the information system, and

the information within it, must first be determined. That is, what elements of information and

information system (IS) capabilities require assurance based upon the associated risks of

compromise, corruption or loss of use. Additionally, the level of assurance attained must often

be balanced with potential reductions in operational capability and the consumption of valuable

resources (e.g. time, money and people). This thesis proposes advancements in the risk assessment methodology and develops a decision support tool to facilitate a three-dimensional, quantitative tradeoff analysis between the level of IA gained by a collection of capabilities, the resulting effect on operational capability, and the resources required for their implementation.

1.3. Problem Approach

Over time, the new technologies (means) offer new opportunities in communication and organizational efficiency; however, new vulnerabilities may also be introduced. Focusing on what aspects of information and information systems are valued by the decision makers can be used to evaluate current performance and proposed improvements to information systems, and even facilitate the development of previously unforeseen alternatives.

Keeney suggests values, not alternatives, should be the primary focus of decision-making. [Keeney, 1994:33] He further defines values as "(fundamental) principles that define all that you care about in a specific decision situation... which are used to evaluate the desirability of any possible alternatives or consequences." [Keeney, 1994:33] Keeney coined the phrase value focused thinking (VFT) to refer to this approach.

A VFT approach analyzes complex problems that have "multiple competing objectives that require consideration of tradeoffs among these objectives." [Kirkwood, 1997:1] In the case of IA, potential tradeoffs exist between the level of assurance attained, how readily available the information or information services are made to the user, and the subsequent implementation costs. Typically, expertise and preferences from owners and stakeholders of the information system would be captured and integrated into the model. However, for this proof of concept phase of study, these inputs were taken primarily from Joint- and Service-specific doctrine.

1.4. Research Scope

The overall perspective of this thesis is from the war-fighter's viewpoint. It is realized that although the governmental and commercial sectors share many common concerns with respect to IA, there are fundamental differences in some areas that may not be captured within the current model.

The growing concerns over the protection, detection and reaction to wide-scale attacks are valid but beyond the scope of this thesis. Considering the 'weakest link' approach, if each individual organization attains the highest level of information assurance possible, then wide-scale protection may be implied. The framework for this effort, however, will bear in mind the follow-on requirement of wide-scale information assurance.

Finally, due to the classification levels of some counterattack capabilities, the scope of retaliatory actions against attacks is limited to the pursuit of legal remedies.

1.5. Assumptions

The methodology utilized in this thesis assumes the following tasks have been accomplished prior to implementation of the decision support tools:

- A vulnerability assessment has been accomplished and results are available;

- Risks have been prioritized based upon their impact and likelihood by a detailed risk assessment, types of which are discussed in Chapter 3; and,

- Countermeasures have been proposed to mitigate the risks identified. These will serve as a starting point in IA strategy development. An IA strategy is defined as a combination of technical (hardware and software) and non-technical (policy and procedure) means to achieve Information Assurance objectives.

1.6. Overview and Format

The structure of this thesis begins with a literature review pertinent to IA, as well as the basic elements of VFT, in Chapter 2. Chapter 3 discusses the value of information, the

quantification of this value using VFT, and the integration of the resulting value model into the

risk management process. Chapter 4 builds upon the output of this process by outlining the

development of a triad of models that evaluate the effectiveness of IA strategies, their impact

upon operational capabilities, and the resources required to implement them. Chapter 5 presents

conclusions derived from the proof of concept research and recommendations for future efforts.

2. Literature Review

There exists a large collection of documents dealing with what IA should be, methods on achieving assurance, and suggested strategies ('defense-in-depth' for example). The following review intended to serve three main purposes:

- Identify the value of information in current and future military endeavors;

- Identify a 'gold standard' (taken primarily from joint and service-specific doctrine) that revealed the true values of military decision makers with respect to information, its uses in military operations, and the assurance of information and information operations; and,

- Provide appropriate background information required to apply value focused thinking to the IA problem.

2.1. Existing Doctrine and Information Assurance

Doctrine, both Joint- and Service-specific, provide an excellent source of objectives critical to senior decision makers. For example, "Air and space doctrine is a statement of officially sanctioned beliefs and warfighting principles that describe and guide the proper use of air and space forces in military operations." [AFDD 1, 1997:1] This generally holds true regardless of the source of doctrine. Encompassed within all levels of doctrine includes the objective of IA, reflecting the senior leaders' perspectives and experience on the relationship between IA and national security. These serve as a potential source of values, from which an overarching model may be constructed.

2.1.1. Cornerstones of Information Warfare

In 1995, the Secretary of the Air Force and the USAF Chief of Staff presented the *Cornerstones of Information Warfare*. The document focused on the strengths and weaknesses of information technologies within Air Force operations. They concluded, "as the Air Force becomes more technologically sophisticated, it becomes more technologically dependent... and

these dependencies represent potentially crippling vulnerabilities." [Cornerstones, 1995:15] The authors also defined Defensive Counterinformation (DCI) as "actions protecting our military information functions from the adversary." [Cornerstones, 1995:Definitions] This white paper served as a prelude to the growing interest of protecting friendly information systems and assuring their future use; the development of Joint doctrine to address these issues followed.

Figure 2-1 illustrates two categories of attacks currently requiring defensive measures: Direct and Indirect Information Warfare. Direct implies an attack upon our information or information systems, changing data in the pursuit of changing perceptions of those using the targeted information. Indirect refers to enemy actions taken to deceive information collection efforts (building a fake runway, for example). Computer, Operations and Communications Security were, at the time, the measures taken to fulfill this mission. It was recognized that advances in information technology required equal advances in these measures, and perhaps warranted new ones.
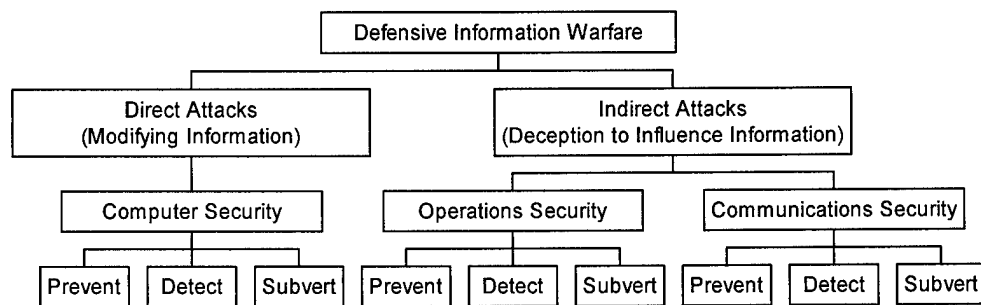
Figure 2-1: Defensive IW [extracted from Cornerstones, 1995]

2.1.2. Joint Publications (JP) 3-13

JP 3-13, entitled *Joint Doctrine for Information Operations*, discusses both offensive and defensive information operations, stating both are equally important to ensure successful military operations. JP 3-13 offers the following, widely accepted, definition of IA.

IA protects and defends information and information systems by ensuring their availability, integrity, identification and authentication, confidentiality, and non-repudiation. This includes providing for the restoration of information systems by incorporating protection, detection, and reaction capabilities. IA employs technologies and processes such as multilevel security, access controls, secure network servers, and intrusion detection software. [JP 3-13,1998:III-1]

Restated, IA ensures that information and information systems are available to decision-makers when needed, that the information is as accurate and complete as possible, and that control over both the information and the information systems is maintained. In the event that control is lost, the capabilities to detect a loss of control, to regain control, and to restore the information systems to its original state must exist. These objectives are achieved by taking proactive measures (to protect) and allowing for detection and reaction capabilities (to defend) through the integration of secure technologies and best practices into the information system. For further clarification, specific definitions of these IA requirements are shown in Table 2-1.

Table 2-1: Definitions of IA Objectives

Definitions of IA Objectives	
Availability	Assured access by authorized users[1]
Integrity	Protection from unauthorized change[1]
Identification	Process an information system uses to recognize an entity.[2]
Authentication	Verification of the originator; Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.[2]
Confidentiality	Protection from unauthorized disclosure[1]
Non-Repudiation	Undeniable proof of participation[1]
1. JP 3-13 2. Air Force Manual (AFMAN) 33-223	

The extent of the measures taken to provide IA for information systems and information-based processes is dependent upon the value of the information contained within and the consequences associated with their compromise or loss of access. Although information has been an important contributor to success in battle, information is now regarded as "a strategic

resource vital to national security." [JP 3-13, 1998:I-18] To complicate matters, the value

placed upon information often changes over time, based upon its usefulness (or lack thereof)

during the changing levels of conflict and phases of an operation. [JP 3-13, 1998:I-5]

The objectives of defensive IO include information environment protection, attack

detection, capability restoration, and IO attack response. [JP 3-13, 1998:ix] Table 2-2 describes

the elements that comprise the information realm.

Table 2-2: Elements of the Information Realm

Information
Facts, data, or instructions in any medium or form. This includes the meaning that humans assign to data by means of known conventions used in their representation
Information-Based Processes
Processes that collect, analyze, and disseminate information using any medium or form, that adds value to the decision making process by performing designated functions or provide anticipated services
Information System
The entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information. The information system also includes information-based processes.
[JP 3-13, 1998:I-9-I-11]

Figure 2-2 illustrates the sub-objectives and related concerns for the four areas within

defensive IO. Information assurance, as implied in Figure 1-1, encompasses defensive IO in the

context that our systems are under continuous scrutiny by varying levels of threats. Although the

concepts of defensive IO and IA are similar, the definition of IA is used to develop a hierarchy of

main objectives. These objectives, defined in Table 2-3, include *Information and Information*

System (IS) Protection, *Detection*, and *Reaction* capabilities.

Defensive IO

Information Environment Protection
- Education & Training
- Risk Management
- Intelligence Support
  - Threat Analysis
- Public Affairs
- Command Information
- Security
  - Personnel
  - Physical
  - Industrial
- Vulnerability Analysis
  - Internal
  - External
  - Accidental Sources
  - Natural Phenomena
- Monitoring Processes
- IA Support
  - INFOSEC
    - COMPUSEC
    - COMSEC
  - Electronic Protect (EP)

IO Attack Detection
- Timely Detection
  - Service Information Warfare Centers
  - Information System Developers
    - Designs Mitigate Vulnerability
    - Designs Incorporate Detect & Report Mechanisms
  - Information System Providers/SysAdmin
    - Recognize & Report Attacks
    - Initiate Mitigation Process
    - Periodic Risk Assessment
  - Users
    - Recognize & Report Abnormalities
  - Law Enforcement Support
  - Intelligence Support
    - Indicator & Warning Processes
- Timely Reporting
  - Reporting Structure
    - Continuously Functioning
    - Adequately Linked

Capability Restoration
- Pre-established Procedures
  - Backup/ Redundant Links
  - Alternative Means of Transfer
  - Automated Restoration
- Computer Emergency Response Teams
- Technical Restoration Capabilities
- Automated Intrusion Detection Systems
- Inventory of Systems Resources
- Post-Attack Analysis

IO Attack Response
- Identify Actors & Intent
- Establish Cause and Complicity
- Apply Deterrent Options
  - Law Enforcement
  - Diplomatic Actions
  - Economic Sanctions
  - Military Force

Figure 2-2: Defensive IO [Doyle, Deckro, Jackson and Kloeber, 1997:36, JP 3-13, 1998]

Table 2-3: IA Objective Definitions

IA Objective Definitions
Information and IS Protection: includes those measures taken to afford protection to information and IS, and ensure their availability, confidentiality, and integrity.
Detection: includes measures taken to provide detection of impending or ongoing attacks against an information system or the residing information.
Reaction: includes the measures taken to (1) appropriately respond to an identified attack and (2) restore the information and IS capabilities to an acceptable state, their original state, or an improved state. [Modified from the definition of IA in JP 3-13]

These capabilities provide value in the sense that if one is missing, any level of assurance cannot be demonstrated. Figure 2-3 shows the top tier of an IA hierarchy, which is developed further in Chapter 4.

```
                        ┌─────────────────────────┐
                        │  Information Assurance   │
                        └─────────────────────────┘
        ┌──────────────────────────┼──────────────────────────┐
┌─────────────────────────┐ ┌──────────────┐ ┌──────────────┐
│Information & IS Protection│ │  Detection   │ │   Reaction   │
└─────────────────────────┘ └──────────────┘ └──────────────┘
```
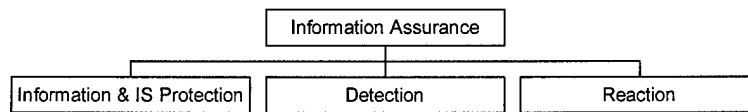
Figure 2-3: IA Value Hierarchy

2.1.3. JP 3-13.1

JP 3-13.1, entitled *Joint Doctrine for Command and Control Warfare (C^2W)*, primarily deals with the offensive aspects of information warfare, which is illustrated in Figure 2-4. However, it does provide some insights into why measures must be taken to protect information systems. In particular, the interconnectedness of information infrastructures and the role that information and information systems serve in the decision-making process are discussed.
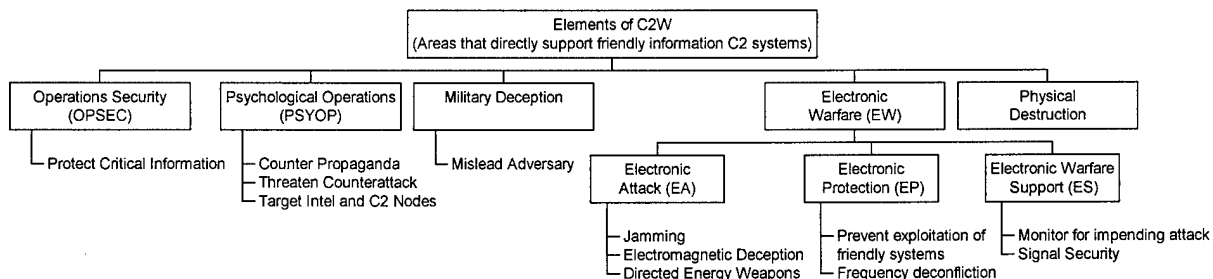
Figure 2-4: Elements of C2W [Extracted from JP 3-13.1, 1996; Doyle, et. al., 1997:43]

The information infrastructures of today may be categorized into three areas: the Global Information Infrastructure (GII), the National Information Infrastructure (NII), and the Defense Information Infrastructure (DII). The GII is "the worldwide interconnection of communications networks, computers, data bases, and consumer electronics that make vast amount of information available to users." [JP 3-13.1, 1996:I-2] The NII is "the nation-wide interconnection of communications networks, computers, databases, and consumer electronics that make vast

amounts of information available to users" and pertains to those assets that reside within the national boundaries. [JP 3-13, 1998:GL-8] Finally, the DII is defined as "the shared or interconnected system of computers, communications, data applications, security, people, training, and other support structures serving the United States' Department of Defense local, national and worldwide information needs." [JP 3-13.1, 1996:I-2] In reality, the boundaries between these infrastructures are merely conceptual, since they are "inextricably intertwined." Thus, an adversary often has a direct, electronic path, to virtually any information system, regardless of its physical location. [JP 3-13.1, 1996:I-3]

The Observe-Orient-Decide-Act (OODA) loop, in the context of command and control, is also discussed in JP 3-13.1. (Figure 2-5) The loop, or decision cycle, begins with *Observe*— comprised of the gathering of information from multiple sources. The second step, *Orient*, requires the decision-maker to assess the perceived *reality* of the operational area based upon the information provided. The accuracy of the decision-maker's perception of reality compared to the actual reality is subject to imperfect processes and systems, as well as adversary actions. Once the decision-maker is oriented and actually makes a decision (*Decide*), those directions are (typically) communicated to subordinate forces. [JP 3-13.1, 1996:A-1; Boyd, 1982]
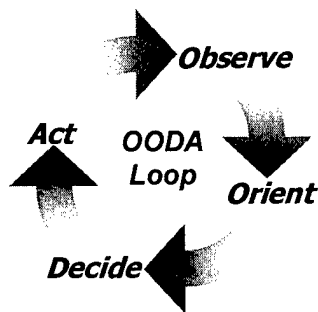
Figure 2-5: OODA Loop [JP 3-13.1, 1996:A-2; Boyd, 1982]

This cycle ultimately results in "the commander's decisions [becoming] actions that impact the reality of the operational area." [JP 3-13.1, 1996:A-1] Essentially, all of these phases are subject to threats. For example, information gathered in the *Observe* phase could potentially be altered, changing the *Orient* and *Decide* results to the enemy's advantage. In addition, the information systems that are relied upon for communication could be denied, resulting in a breakdown in the decision cycle altogether.

Information is necessary in supporting decision-making. The potential for an adversary to affect any part of the OODA loop, or the information infrastructures, upon which the military heavily relies, further justifies the need for information assurance.

2.1.4. AFDD 1 – Air Force Basic Doctrine

Building upon the principles of war discussed by J. F. C. Fuller (Offensive, Mobility, Surprise, Concentration, and Protection), Air Force Basic Doctrine shapes the manner in which the Air Force operates, and provides a common set of understandings and principles upon which airmen make military decisions. [AFDD 1, 1997:1; Fuller, 1992:48-52] This document, fundamental to the US Air Force, illustrates the importance of the role that information operations and technologies play within the context of modern and future warfare, particularly within the air and space power functions and the principles of war, through the concept of *Information Superiority*.

> "Information superiority is the ability to collect, control, exploit, and defend information while denying an adversary the ability to do the same and, like air and space superiority, includes gaining control over the information realm and fully exploiting military information functions. Information superiority was the first function of the Air Force. Early balloons and airplanes became spotters for Army commanders who wanted information in order to gain an advantage over an adversary and improve their decisions on the battlefield. Today, the Air Force is the major operator of sophisticated air- and space-based intelligence, surveillance, and reconnaissance systems and is the Service most able to quickly respond to the information they provide." [AFDD 1, 1997:31]

Figure 2-6 illustrates the main functions of *information superiority*. Information and information technologies are playing greater roles in the accomplishment of national, and subsequently military, objectives.
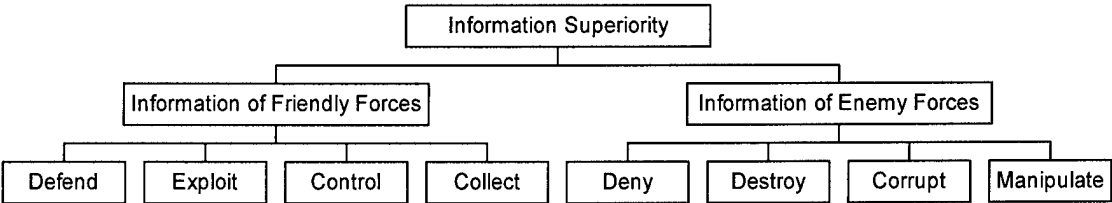
Figure 2-6: Information Superiority [Extracted from AFDD 1, 1997]

Information and information technology pervade the principles of war, listed in Table 2-4, and promises new and improved capability, efficiency, lethality, and deterrence.

Table 2-4: Principles of War [AFDD 1, 1997:12; Fuller, 1992:48-52]

Principles of War	
Unity of Command	Economy of Force
Objective	Security
Offensive	Surprise
Mass	Simplicity
Maneuver	

Today's forces rely heavily upon information and information technologies to enhance their capability to exercise these principles of war and to achieve military objectives. A summary of the relationships and the impact of the 'Information Age' upon these principles follow.

Unity of Command, Objective & Offensive

As noted above, information has historically played an important role in improving the decisions made on the battlefield and gaining advantages over a less aware enemy. Information that is accurate, usable, and not overwhelming increases the speed and quality of one's Observe-

Orient-Decide-Act (OODA) loop. If one protagonist has an advantage in timely and accurate decision-making, the other will suffer, due to reactive stress. To further the advantage, if one can degrade the timeliness and quality of an enemy's decision process, there also exists the capability to shape the adversary's perception and subsequent actions. [AFDD 1, 1997:32]

Mass

This principle requires the proper concentration of combat power at the decisive time and place. [AFDD 1, 1997:15] In the past, *mass* involved enormous barrages that dropped tons of explosives on or around a potential military target. Today, information technology provides precision guided weapons and "superior battlespace awareness," replacing brute force tactics, and presents "new opportunities to attack critical targets... with precision, stealth, and the speed of light, affecting a variety of functions and capabilities." [AFDD 1, 1997:15-16]

Maneuver & Economy of Force

Information and communications systems facilitate the management of massive volumes of force deployment and shifting supply inventory data. The resulting efficiencies have become essential to maintaining support operations with today's smaller force and support structures. [AFDD 1, 1997:34]

Security

The principle of security "conceals friendly capabilities and intentions while allowing our forces the freedom to gather information on the adversary." [AFDD 1, 1997:19] Once again, the heavy reliance upon information technology now requires that securing the information realm is equally important to that of maintaining physical security. The forces with "the best ability to gain, defend, exploit, attack information, and deny the same capabilities to an opponent, has a distinct strategic advantage." [AFDD 1, 1997:19-20]

Surprise

Information technologies, when combined with stealth and situational awareness superior to that of the enemy's, can provide shock and surprise to avoid unnecessary exposure of friendly forces. [AFDD 1, 1997:20]

Simplicity

Information technologies support the eventual goal of information superiority to allow faster, and more effective command and control capabilities than the adversary. However, this does not imply more information, but instead suggests information that is accurate, usable, and in the appropriate context and amount. [AFDD 1, 1997:31-32]

Summary

The nature of the threats, and the methods to counter them, are evolving. Endeavors to gain global awareness, to facilitate command, control and communication rest on the ability to provide security and guaranteed access to information and information systems. [AFDD 1, 1997:44]

2.1.5. Information Technology for the 21st Century (United States Navy)

This article summarizes the revolutionary approach the United States Navy is taking with information technology, particularly in the area of command and control. Communications within the naval forces has evolved from "flags and flashing lights to secure radios to e-mail." [Clemins, 1997:67] The initiative "Information Technology for the 21st Century," nicknamed IT-21, plans to "shape warfighting capabilities, support systems, and information processing. In fact, information sharing (and knowledge sharing) already dominates the relationship of the Navy with the Army, Marines, Air Force and allies." [Clemins, 1997:67] Not unlike the other branches of the Armed Services, the Navy's shrinking force levels and budgets necessitate a

greater reliance upon joint operations to fulfill national objectives. The Navy foresees a future with fewer sailors operating systems that are more capable and subsequently performing a greater number of missions. [Clemins, 1997:68] IT-21 is a method to identify opportunities for greater efficiencies and force enablers, and is based upon seven precepts.

(1) Leadership must lead the implementation of new technology, and be aware of its benefits and disadvantages before allocating already scarce resources.
(2) Integrate tactical and tactical support areas; explicitly, fight and run ships from a single PC-based system.
(3) Rely heavily upon industry standards to stay abreast of technology and avoid incurring research and development costs.
(4) Drive everything to a single PC, utilizing a client-server environment using off-the-shelf software.
(5) Use commercial off-the-shelf (COTS) products for almost everything, and streamline the way these products are purchased and managed.
(6) Seamless transition from shore to sea; "A ship in San Diego, connected via fiber-optics on a pier to the metropolitan area network, must get underway and switch to satellite so that it is completely transparent to the user."
(7) Focus on software applications to comprise the C4I architecture instead of the tailored hardware and software used in the past. "Buy icons, not hardware." [Clemins, 1997:68]

During a 1997 test of IT-21 concepts (Fleet Battle Experiment ALFA), "web pages and e-mail were used to rapidly and routinely transmit information and knowledge—classified and unclassified, tactical and tactical support. This dramatically increased the speed of command and compressed the time required for coordinating events." [Clemins, 1997:69]

This approach to taking total advantage of current IT has formed the concepts of virtual command posts and enhanced data fusion capabilities, and offers tremendous potential in methods of disseminating information. However, IA of these systems is crucial in maintaining these systems, their function, and the capability of the United States Navy.

2.2. Other Government Studies

2.2.1. RAND – Defensive Information Warfare

This text clarifies areas of defensive operations within IW, an approach closely related to

tackling the problem of IA. This approach formulates the defensive IW problem as

> "... the possible environments that may be faced, one's options, and the
> objective that is being sought. This requires an identification of the variables that
> are relevant, that is, those that can significantly influence the outcome as well as
> the subset of these relevant variables that are controllable, which form the basis of
> designing options." [Alberts, 1996:19]

This formulation connotes a vulnerability assessment of systems of interest.

Alberts notes that understanding the threats applicable to a system is a crucial first step in

developing an effective defensive IW strategy. A threat topology is developed and is comprised

of a multidimensional threat with varying abilities to impose varying consequences. Three

categories were defined as *Everyday*, *Potentially Strategic*, and *Strategic*, ranging from the

potential for isolated/limited interruptions to catastrophic amounts of damage. In order to

counter these threats, Alberts discusses the 'defense in depth' method of protecting information.

Defense-in-depth is "a strategy that involves a series of successively stronger or 'higher'

defensive barriers that work together to decompose the spectrum of threats into manageable

pieces." [Alberts, 1996:39] The "lines of defense" are directly correlated to the categories of

threats discussed earlier. As the level of threat increases, so does the sophistication of the

defensive barriers. The depth also provides a means to "concentrate intelligence and monitoring

efforts on a smaller population, which in turn increases the chances of successful defense."

[Alberts, 1996:40]

System defense extends beyond the proper implementation of design and software quality

assurance. Alberts contends that defensive capabilities include "system operations, methods, and

procedures employed to limit the attractiveness of an attack and/or the consequences of an

attack," some of which are shown in Figure 2-7. [1996:70] These dimensions are 'tuned'

according to system-specific circumstances and operational considerations, resulting in a desired

level of more (or less) protection. The author noted, "More protection always comes at a

price..." either costing more to build a system or exacting "costs in terms of overhead or in loss

of functionality." [Alberts, 1996:70-71]

Dimensions of Defense

Control Access	Control Activity	Limit Value	Detect/Limit Attacks	Limit Damage	Limit Disruption
Deny	Deny	Fully Encrypt	Active System Monitoring	Deny	Multiple, Automated Alternatives
Screen	Set Limits	Commercial Encrypt	Monitor Specific Threats	Periodic Backup	Limited Alternatives
Password	Authenticate	Simple Codes			Few Alternatives
Open	Open	Open	React	None	None

Figure 2-7: Dimensions of Defense [Alberts, 1996:72]

Finally, Alberts noted five challenges to defensive information warfare capabilities that

remain strong today. These included:

- A better understanding of the nature of the threat must be achieved;
- A deterrent strategy against digital attacks must be developed;
- Timely notification of indicators and warning regarding impending attacks;
- Methods for successfully defending against attacks that do occur; and,
- The development of "appropriate and effective responses to attacks." [Alberts, 1996:59-62]

2.2.2. RAND – Securing the US DII: A Proposed Approach

Anderson, Feldman, Gerwehr, Houghton, Mesic, Pinder, Rothenberg, and Chiesa define

the minimum essential information infrastructure (MEII) as a process, rather than a structure. A

methodology to attain a feasible MEII is proposed, and the concept is described by the following

four principles. The MEII...

- Does not guarantee security but is instead a type of information system insurance policy by which risks are managed at some reasonable cost while pursuing information age opportunities;

- Is not a central system responding to multiple threats but a set of systems defined locally to respond to local vulnerabilities;

- Is not a fixed, protected entity, but a virtual functionality on top of the existing infrastructure; and

- Is not a static structure, but a dynamic process—a means to protect something, instead of a thing that has to be protected. [Anderson, et. al, 1999:xiv]

The focus is on military organizations, and it is assumed that as more organizations

complete this process, an MEII will evolve, thus securing the defense information infrastructure

(DII). This is in agreement with the 'weakest link' approach to security in general.

The process they define has six steps shown in Figure 2-8.

1.	Determine what information functions are essential to successful execution of the unit's missions.
2.	Determine which information "systems" are essential to accomplish those functions.
3.	For each essential system and its components, identify vulnerabilities to expected threats. In analyzing the system, it could (and perhaps should) be viewed in various ways: as a hierarchical set of subsystems supporting each other at different levels, or as a collection of functional elements like databases, software modules, hardware, etc.
4.	Identify security techniques to mitigate vulnerabilities.
5.	Implement the selected security techniques.
6.	Play the solutions against a set of threat scenarios to see if the solutions are robust against likely threats. It is critical that the success of security enhancements be testable.

Figure 2-8: Six Steps of the MEII Process [Anderson, et. al., 1999:xiv-xv]

Generic sources of vulnerability are identified to facilitate analysis. In addition, a matrix

tool is developed to ascertain the effectiveness of certain countermeasures against identified

vulnerabilities, as well as any additional vulnerability that may be incurred due to using the new

countermeasure. The 'ranking' used is a color-based scale that indicates both the level a

countermeasure addresses an existing vulnerability and the level of new vulnerability a
countermeasure may impose if implemented.

The overall process is similar to other risk reduction or risk assessment processes. With
the exception of identifying 'essential' functions and systems, there appears to be no direct
connection between the value of information and the 'value added' by implementing a
countermeasure. However, categories of security techniques, shown in Table 2-5, may illustrate
desirable attributes of an information system in the context of information assurance.

Table 2-5: MEII Security Technique Categories [Anderson, et. al., 1999:xvii]

Heterogeneity	May be functional (multiple methods for accomplishing an end), anatomic (having a mix of component or platform types), and temporal (employing means to ensure future admixture or ongoing diversity).
Static resource allocation	The *a priori* assignment of resources preferentially, as a result of experience and/or perceived threats, with the goal of precluding damage.
Dynamic resource allocation	According some assets or activities greater importance as a threat develops; this technique calls for directed, real-time adaptation to adverse conditions.
Redundancy	Maintaining a depth of spare components or duplicated information to replace damaged or compromised assets.
Resilience and robustness	Sheer toughness; remaining serviceable while under attack, while defending, and/or when damaged.
Rapid recovery reconstitution	Quickly assessing and repairing damaged or degraded components, communications, and transportation routes.
Deception	Artifice aimed at inducing enemy behaviors that may be exploited.
Segmentation, decentralization, and quarantine	Distributing assets to facilitate independent defense and repair; containing damage locally and preventing propagation of the damaging vector.
Immunologic identification	Ability to discriminate between self and non-self; partial matching algorithms (flexible detection); memory and learning; continuous and ubiquitous function.
Self-organized and collective behavior	Valuable defensive properties emerging from a collection of autonomous agents interacting in a distributed fashion.
Personnel management	Personnel security clearances and training, design of human interfaces to reduce vulnerability of systems to human frailties.
Centralized management of information resources (Self explanatory)	
Threat/warning response structure	Establishment of a hierarchy of increasing information attack threat levels and concomitant protective measures to be taken.

2.2.3. RAND – Countering the New Terrorism

Lesser, Hoffman, Arquilla, Ronfeldt and Zanini discuss the evolution of terrorism, particularly its improving lethality and the implementation of information technologies to organize and enhance traditional and new forms of hostile acts. Netwar "refers to an emerging mode of conflict and crime at societal levels, involving measures short of traditional war, in which the protagonists use network forms of organization and related doctrines, strategies, and technologies attuned to the information age." [Lesser, et. al., 1999:47] This prospect of network-based conflict and crime is expected to become major phenomena in the decades ahead. "Various actors across the spectrum of conflict and crime are already evolving in this direction. Examples include… the Middle East's Hamas, Mexico's Zapatistas, and the American Christian Patriot movement, to name a few." [Lesser, et. al., 1999:47]

Not unlike the Air Force's ability to control and conduct coordinated attacks from multiple geographic locations, terrorist organizations using similar information technology to their advantage poses a major problem in "correct identification of the enemy." [Lesser, et. al., 1999:xii] Even if the adversary is identified, the authors note that the 'effectiveness' of military force as a deterrent is problematic due to the potential for unintended consequences (e.g. friendly casualties or damage to world opinion). [Lesser, et. al., 1999:xii]

2.2.4. The Cyber-Posture of the National Information Infrastructure

"Critical Infrastructure Protection (CIP) is that portion of the national infrastructure which is considered most critical to national interests and, therefore, requires protection against cyber- and other attacks." [Ware, 1998:5] Ware offered several actions that would aid in strengthening the cyber posture of the NII, four of which are directly applicable to this research. These include:

- The US government should organize to improve its information security posture expeditiously, directing agencies to bring the security status of their information systems up the be best current practice; agency response and progress should be monitored. This implies that organizations and their information systems require a certain level of compliance.

- Assess the physical vulnerability of the infrastructure, especially the telecommunications and computer system dimensions. It was noted that telecommunications redundancy tends to mitigate, but not eliminate, physical weaknesses.

- Assess the present level of computer/network security throughout the private sector.

- Develop a roster of currently existing "early warning mechanisms" that could contribute to a national alerting and monitoring center. [Ware, 1998:34-35]

Ware argues that increasing levels of automation results in fewer people who know how to run systems "the old way," thereby increasing the vulnerability associated with cyber attacks due to the potentially inadequate preparation or non-existent backup procedures. Tradeoffs must be made regarding the advantages of automation and the potential for "accidental and deliberate failures in automated systems." [Ware, 1998:9]

Sources of such failures were categorized as disruptive phenomena, infrastructure noise, moderate and low-level CIP attacks and intrusions, extremely high-level attacks and intrusions, and physical attacks. [Ware, 1998:11-14] Disruptive phenomena are defined as natural phenomena, carelessness, accidents and oversights that "cause disruption to smooth system and overall operation, dislocation of delivered services, or force annoyances on end-users." [Ware, 1998:9] Infrastructure noise, a similar concept to engineering noise, is defined as "unintended spurious events that occur daily throughout the national infrastructure." [Ware, 1998:10] This noise, however, may potentially mask deliberate offensive attacks—"a nuisance for the defense; and an exploitable feature for the offense." [Ware, 1998:11] Ware defines low-level attacks as those that approximate the infrastructure noise level, and are remedied by in-place measures. Medium-level attacks are those that "exceed the consequences of routine events, [where] the response mechanisms that have been developed and have evolved can be stretched and

2-18

supplemented by ad hoc arrangements and actions." [Ware, 1998:12] Extremely high level attacks and intrusions as those "extensive enough to disrupt or destroy the functioning of very large geographical areas or bring down most of a major industry." [Ware, 1998:13] Finally, physical attacks are those actions taken against the physical components of any part of the infrastructure. [Ware, 1998:14]

The interconnectedness of infrastructures means that sectors can support others by providing services, computing support and computer-based functions, data, utilities, and perhaps combinations of these (directly and indirectly). [Ware, 1998:15] The failure of one sector could have tremendous impacts upon all subsequently reliant sectors. This indicates the need for not only evaluating an organization's physical and cyber posture, but the related organizations upon which it sustains and relies upon.

However, Ware asserts that the inherent resilience built into our infrastructure (as a result of the size of the country, the preparedness of individual organizations, the artifacts of the cold-war build-up and military readiness) can offer some capability to mitigate infrastructure noise and low-level attacks. [Ware, 1998:23-24] In addition, "it follows that, for limited spans of time, the country can make do without—or with impaired—sector(s) of the normal infrastructure." [Ware, 1998:25] Nonetheless, this should not foster complacency. The increasing openness of computer systems in the pursuit of enhanced service and improved access exposes them to a broader threat spectrum and an increased likelihood of suffering a cyber attack. [Ware, 1998:30]

2.3. New World Vistas

The USAF Scientific Advisory Board (SAB) addressed the potential requirements necessary to achieve a set of goals for 21st century aerospace power. These goals included:

- Get the right knowledge, to the right place, at the right time for all aerospace missions;

- Protect all Air Force computers, software, and data, regardless of platform or location, particularly those involved in warfighting;

- Achieve global communication between the air, ground, and space assets of the AF, as well as those with whom we operate;

- Maximize the speed and quality of AF coordination, planning, and execution;

- Dominate the information battlespace; and,

- Develop doctrine needed for the use of information in dynamic command and control of joint forces.

The omnipresent element of information and information technologies will enable and enhance the accomplishment of these goals. However, the study also noted that the Information Revolution is accompanied by new threats to the Air Force and the cyberspace relied upon for mission execution.

The authors noted that cyberspace is essential to Air Force mission execution and therefore requires protection. This protection, however, goes beyond "normal security considerations... not only including the AF assets, but also its access to commercial infrastructure and in some cases protect the infrastructure itself." [SAB, 1995:17] This protection was thought to be required in two dimensions: data and control.

Data, "a sequence of bits to which meaning may be assigned, must be protected from unauthorized disclosure and from corruption or loss." Control, "the process that has execution authority of a computer system, must be protected from unauthorized users and from automated attacks." [SAB, 1995:20] The authors further stated that these dimensions must be protected in bounded and unbounded systems, differentiated by the existence or nonexistence of a "central or distributed authority (common administrative control) over all components of the system" respectively. [SAB, 1995:21] The intermingling of these types of systems opens up potential vulnerabilities, due to the lack of a full understanding of the relationships between them, and the

lack of protection between the two. Table 2-6 summarizes the threats discussed and the potential

countermeasures to mitigate them.

Table 2-6: Threats and Countermeasures [SAB, 1995:22]

Dimension/System	Threats	Countermeasures
Data/Bounded	Disclosure Loss of integrity	Data encryption & access control Crypto checksums
Data/Unbounded	Disclosure Disclosure in transit Loss of integrity Exploitation of traffic analysis	Authorization & authentication Data encryption Data encryption Future capabilities
Control/Bounded	Trojan Horse Viruses Exceeding authority	Strong policy & procedure Limited detection prevention Accounting & logging
Control/Unbounded	Worms Corrupted agents Intrusions	Limited detection prevention Docking protocols User proxy firewalls

Other threats that were acknowledged, but not discussed included denial of access

attacks, the exploitation of communications links, and Trojan Horses embedded within

commercial products in defense systems—all of which are in existence today. [SAB, 1995:29]

Recommendations made by the SAB included the requirement for impenetrable core

systems, an Information Warfare bias toward protection and not attack, and multidimensional

protection all maintain the need for an effective IA strategy.

2.4. Relationships of Information to IW

"The bad news is that all of the hype [about information warfare] could
impede sensible policy analysis, cloud objective resource allocation decisions,
and mask real technical and operational risks and vulnerabilities. In the scramble
for turf and budget shares, clear thinking about the relative value of information,
in all of its various dimensions and implications for the U.S. military, has too
often been a casualty. That could lead to unfortunate structural changes in
organizations, inadequate analysis of critical issues, and a failure to prioritize
effectively in applying information technology to warfare and broader national
security concerns." [Buchan, 1996]

As Buchan stated, "the relative value of information" to its government and civilian owners lacks explicit definition. Many studies and programs address the underlying issues of IA, commonly citing a 'defense-in-depth' approach to achieving a reasonable level of IA, given some tradeoffs in performance (speed in particular) and accessibility to information, and assuming that known vulnerabilities are remedied. A 1996 study by the Office of the Under Secretary of Defense for Acquisition & Technology recommended the following steps in evaluating the area of defensive IW (which generally also apply in times other than crisis).

- Identify the information users of national interest who can be attacked through the shared elements of the national information infrastructure.

- Determine the scope of national information interests to be defended by information warfare defense and deterrence capabilities.

- Characterize the procedures, processes, and mechanisms required to defend against various classes of threats to the national information infrastructure and the information users of national interest.

- Identify the indications and warning, tactical warning, and attack assessment procedures, processes, and mechanisms needed to anticipate, detect, and characterize attacks on the national information infrastructure and/or attacks on the information users of national interest.

- Identify the reasonable roles of government and the private sector, alone and in concert, in creating, managing, and operating a national information warfare-defense capability. [Andrews, 1996:i]

This study generated a 'laundry list' of steps to take during times of hostile activities. It is important to note that many of these actions are required well before the initiation of hostilities, due to the time and fiscal investments required, further justifying the need for the ever-present information assurance.

2.5. Risk Management

The *Accreditor's Guideline* written by the National Computer Security Center (NCSC) provides guidance on the certification and accreditation process required for DOD information

systems. Within this document, the risk management process is described. This process allows decision-makers to focus on the elements of their systems that require the most information assurance. Risk is "something bad that might, or might not, actually come to pass." [Kirkwood, 1997:136]

The notion of risk avoidance—"the view that all risks to the information of an information system or network ought to be removed entirely before that system was allowed to operate"—was once supported by security professionals. [NCSC, 1997:3-1] Eventually, it was recognized that some level of risk will always remain, and therefore, tradeoffs between security and functionality must be made. [NCSC, 1997:3-2] The current process of risk management approximates the current level of risk within a given system, and relies upon rational decision making to determine if it is at an acceptable level. This guidance identifies two fundamental activities that comprise this process:

- Identification of the security posture (i.e., threats and vulnerabilities) of the system; and,

- Evaluation of the non-technical aspects of the operational posture (i.e. the need for the system to be operational). [NCSC, 1997:3-2]

The security posture helps to identify the likelihood of a vulnerability being exploited; whereas, the operational posture essentially evaluates the value of the information contained within the system, as well as the value that information system capabilities provide to the decision making process. The overall objective is to facilitate the cost-effective placement of countermeasures to mitigate the identified risks.

2.6. Assessing the Value of Information Technology

Of the correlations between business and military organizations, the limited availability of resources, particularly money, is the most common.

"The increasing complexity and magnitude of investments associated with enterprise-wide computing and higher levels of organizational integration. Complex and expensive systems frequently involve lengthy approval cycles and greater difficulty in evaluating the benefits of such investments." [Materna, 1992:2]

This study examined the evaluation processes of "next generation Information Technology investments..." and found that a variety of measures existed, but few ascertained the contributions that the investment made to the "business needs of the firm, however they are defined." [Materna, 1992:2]

The difficulty lies within the measurability of the benefits (and possibly the indirect costs) an IT investment may yield. Two types of benefits "Hard" and "Soft" are discussed and are differentiated by their ease of quantification. *Hard* benefits "refer to those benefits that can be readily quantified using standard measurement techniques," which includes dollars saved or generated, as well as time saved. [Materna, 1992:3] *Soft* benefits "refer to those benefits which are often less obvious or difficult to quantify such as worker empowerment, flexibility, or the multifarious aspects of competitive advantage." [Materna, 1992:3] These are also referred to as *financial* and *operational* benefits, respectively. Three general approaches to measuring these benefits of IT investments are discussed: Economic, Cost Reduction, and Strategic.

Economic approaches include the time-honored analyses such as Net Present Value, Internal Rate-of-return, Return on Investment, and Breakeven/Payback. Unfortunately, these lend themselves to short-term and financially oriented assessments of stand-alone systems, but pose significant weaknesses when applied to long-term, interdependent systems that may involve intangible cost or benefits. [Materna, 1992:4]

The cost reduction approaches discussed include cost displacement/avoidance, work value analysis, and the cost of quality. Cost displacement (or cost avoidance) compares "the cost

of the proposed system to the cost it will displace and avoid." [Materna, 1992:4] Work value analysis assumes that the workload currently placed upon the organization exceeds its capabilities and that "profitable business opportunities are not being exploited for lack of available time." [Materna, 1992:5] Therefore, the work functions are restructured for improved efficiency and effectiveness, allowing the appropriate level of work to be accomplished "faster, better, and cheaper." [Materna, 1992:5] The last cost reduction approach discussed, the cost of quality, asserts that the most effective way to increase profitability is by cutting the costs associated with poor quality processes. [Materna, 1992:6]

Strategic approaches evaluate complex IT investments with wide-ranging influences. Of particular interest are the option value and technical importance measures. Option value takes a decision-tree approach to determine the options a decision-maker has in the future, given the choices she or he makes now. Analyses of the available positions and their relative advantage, or disadvantage, can be used to pick the best long-term strategy. Technical importance evaluates potential investments by their ability to support the achievement of long-term objectives. Although there may be no return on the investment, future operations may be impossible without it. [Materna, 1992:7-8]

In the context of this article, these methods focus on justifying the acquisition of a particular IT investment based upon its advantages and costs alone, and does not include issues regarding information assurance (or the lack thereof). However, these "cost" concepts may be applied to evaluation measure development and provide insight regarding similar tradeoffs between human efficiency, technological efficiency, and today's restrictive hold on resources.

2.7. Value Focused Thinking

2.7.1. Introduction

"Operations research is intended to improve decision making; and values, indicating what one wants to achieve, are essential for guiding decision making." [Keeney, 1994:793] Keeney contends that people want "...better, rather than worse, consequences and better and worse are based on values. Values are what we fundamentally care about in decision-making. Alternatives are simply means to achieve our values." [Keeney, 1994:793]

This focus on values aids in the evaluation of complex decisions—how to achieve an acceptable level of IA, with a minimum operational impact, at a reasonable cost is the complex decision addressed in this thesis. This value focused thinking (VFT) approach "essentially consists of two activities: first deciding what [the decision maker] wants and then figuring out how to get it." [Keeney, 1998:4] However, Keeney defines the typical approach used by most organizations as "alternative-focused thinking," which consists of evaluating the alternatives available and choosing the best one. [Keeney, 1998:4] Even in the alternative-focused approach, the effort of choosing an alternative involves the underlying values of the decision maker, and the best alternative is chosen based upon "the relative desirability of consequences [which] is a concept based on values. Hence, the fundamental notion in decision making should be values, not alternatives." [Keeney, 1998:3] Because of this focus on values rather than alternatives, VFT has been used in this study.

2.7.2. Overview of Value Model Development

A value model is a hierarchical collection of a set of fundamental objectives applicable to the decision problem. These objectives are broken down until they can be measured, allowing

the decision-maker (DM) to quantitatively assess the degree to which these objectives are met.

The desirable properties of these objectives are shown in Table 2-7.

Table 2-7: Properties of Fundamental Objectives

Desired properties of the set of fundamental objectives	
Essential	To indicate consequences in terms of the fundamental reasons for interest in the decision situation
Controllable	To address consequences that are influenced only by the choice of alternatives in the decision context
Complete	To include all fundamental aspects of the consequences of the decision alternatives
Measurable	To define objectives precisely and to specify the degrees to which objectives may be achieved
Operational	To render the collection of information required for an analysis reasonable considering the time and effort available
Decomposable	To allow the separate treatment of different objectives in the analysis
Non-redundant	To avoid double-counting of possible consequences
Concise	To reduce the number of objectives needed for the analysis of a decision
Understandable	To facilitate generation and communication of insights for guiding the decision making process
Source: [Keeney, 1998:82]	

The objective hierarchy begins with top-level objectives, and breaks them down into sub-objectives. This process, called *specification*, "subdivides objectives into lower-level objectives of more detail, thus clarifying the intended meaning of the more general objective." [Keeney and Raiffa, 1993:41] These lower level objectives "may be thought as the means to an end, the end being the higher-level objective." [Keeney and Raiffa, 1993:41] The process continues until the objectives (or sub-objectives) are broken down such that attributes can be identified to measure achievement. Bottom-up analysis ensures lower-level objectives are correctly specified and support the overall objective of the decision. Top-down analysis ensures that the attributes have been sufficiently specified, and helps to determine "where to stop the formalization by considering the advantages and disadvantages of further specification." [Keeney and Raiffa, 1993:43]

2.7.3. Measuring the Attainment of Objectives

In order to assess how well an alternative does, or does not, meet a decision-maker's objectives, a "measuring scale for the degree of attainment of an objective is developed"—defined as an evaluation measure. Kirkwood defines four categories of scales, each with advantages and disadvantages, as a combination of either *natural* or *constructed* and either *direct* or *proxy* methods of measurement. [1997:24]

Generally accepted scales with a common interpretation are *natural* scales and typically take the least time to develop. An example would be measuring cost with dollars. *Constructed* scales are those developed for particular decisions. An example related to information would include classification levels (i.e. unclassified, secret, and top secret). *Constructed* scales fill the void where natural scales are unavailable or inappropriate. "A *direct* scale directly measures the degree of attainment of an objective, while a *proxy* scale measures the degree of attainment of an associated objective." [Kirkwood, 1997:24] *Natural-direct* scales are generally the least controversial, whereas *constructed-proxy* scales must be explicitly defined in order for them to be useful in correctly scoring the attainment a particular alternative may contribute.

Once the scales are developed, the ranges of evaluation must then be defined. This information will permit the logical quantification of the relative importance, and allow the development of the single dimensional value functions. [Keeney, 1994:797]

2.7.4. Single Dimensional Value Functions

Once the ranges and a scale have been determined, the assessment of value for that dimension must be assessed. A single dimensional value function is a monotonic (increasing or decreasing) function, that captures the value a particular score represents to the DM, and is

denoted by *v(x)*. These functions may be discrete, piecewise linear, or continuous, as shown in Figure 2-9 and Figure 2-10 respectively. [Kirkwood, 1997:64-65]
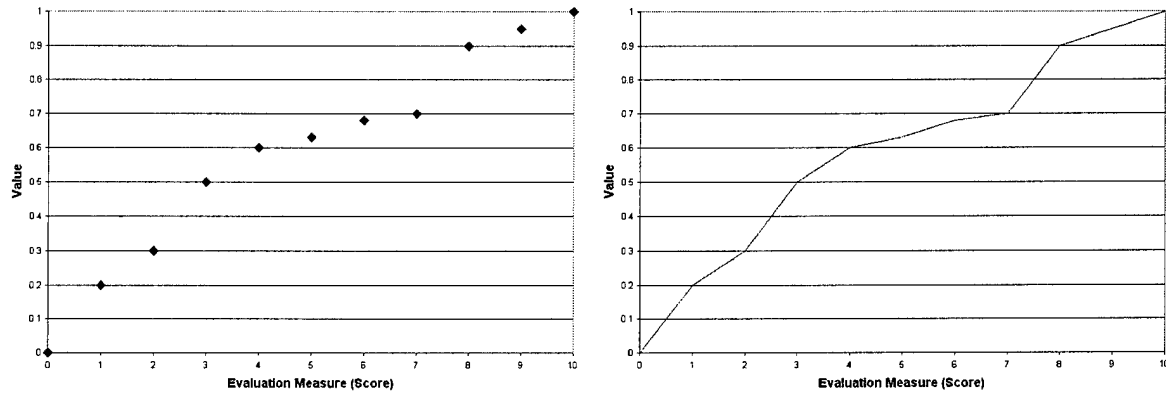
Figure 2-9: Discrete and Piecewise-Linear Value Functions

The degree to which the DM prefers a higher score to a lower score level, termed a *value increment*, is elicited to build the form of discrete or piecewise linear functions. However, the infinite number of scores on a continuous function may require an approximation of the functional form. This procedure relies upon the exponential mathematical function, and one value—the mid-value point—is elicited from the DM. The mid-value point essentially determines the exponential constant, ρ, which is then used in one of the following equations, given by Kirkwood. [1997:65-66]

$$v(x) = \begin{cases} \dfrac{1 - \exp[-(x - Low)/\rho]}{1 - \exp[-(High - Low)/\rho]}, \rho \neq \infty \\ \dfrac{x - Low}{High - Low}, otherwise \end{cases}$$

Equation 2-1: Monotonically Increasing Exponential Single Dimensional Value Function

$$v(x) = \begin{cases} \dfrac{1 - \exp\left[-(High - x)/\rho\right]}{1 - \exp[-(High - Low)/\rho]}, \rho \neq \infty \\[2mm] \dfrac{High - x}{High - Low}, otherwise \end{cases}$$

Equation 2-2: Monotonically Decreasing Exponential Single Dimensional Value Function
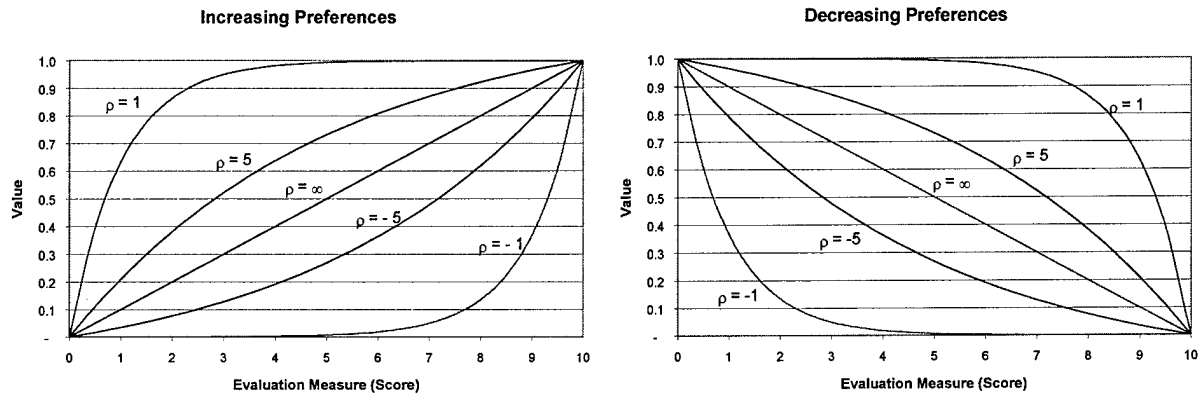
Figure 2-10: Exponential (Continuous) Value Functions

Close inspection of either Equation 2-1 or Equation 2-2 reveals that no closed form solution is available to determine ρ. Therefore, spreadsheet implementation of 'goal seek' was used to determine the value of ρ that would make the appropriate equation, given a value of x and the ranges of the evaluation measure, equal to 0.5, referred to as the mid-value point.

Single dimensional value functions are developed for all evaluation measures within the hierarchy. Once this is done, the preferences between objectives must be elicited from the DM.

2.7.5. Normalized Additive Value Function

A multi-objective value analysis requires a value model that "combines the multiple evaluation measures into a single measure of the overall value of each alternative" under consideration. [Kirkwood, 1997:53] This model is comprised of two main concepts: (1) *Single dimensional value functions*—specified for each evaluation measure; and, (2) *weights*—specified for each *single dimensional value function.* [Kirkwood, 1997:53] The weights are assessed

locally through pair wise comparison of value tradeoffs between evaluation measures, and then are converted to a global perspective by multiplying the local weights down the hierarchy. A notional example highlighting the difference is shown in Figure 2-11.
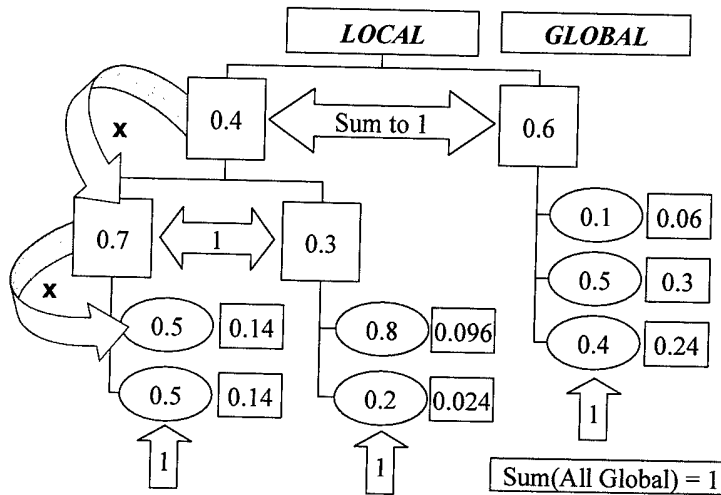
Figure 2-11: Local versus Global Weights

In order to normalize the resulting overall score, the sum of the weights must equal to one. The resulting model, given in Equation 2-3, is defined as the additive value function.

$$v(x) = \sum_{i=1}^{n} \lambda_i v_i(x_i)$$

Equation 2-3: Additive Value Function

Where,

- $\sum_i \lambda_i = 1$ is the requirement for normalization;
- n is the number of objectives (or the number of single dimensional value functions);
- λ_i is the *global* weight for the ith objective;
- $v_i(x_i)$ is the value of the alternative with respect to the ith objective; and,
- $v(x)$ is the overall value of an alternative.

This methodology assumes that the outcomes of each alternative, with respect to their appropriate evaluation measure scores, are deterministic. However, similar to Doyle's

2-31

methodology pertaining to offensive IO evaluation, the expected value, and projected high and low scores may offer an alternative to uncertainty analysis. [Doyle, 1998; Doyle, et. al., 2000]

2.7.6. Sensitivity Analysis

To evaluate the underlying assumptions of the value model, sensitivity analysis may be performed. One of the assumptions often of interest is the weighting of the model. "These weights represent the relative importance that is attached to changes in the different evaluation measures, and this is sometimes a matter of disagreement among the various stakeholders for a particular decision." [Kirkwood, 1997:82] This analysis process is accomplished by varying the weight of interest, while keeping the original ratios of relative importance of the other weights intact, and maintaining the condition that the sum of all weights equal to one. The result shows how the weights affect (or fail to affect) the order of the alternatives, indicating either a sensitive (or insensitive) model.

As an example, using the IA value model shown in Figure 2-12, let the sets (w_p^o, w_d^o, and w_r^o) and (w_p, w_d, and w_r) represent the original and new weights for *Information and IS Protection*, *Detection* and *Reaction* respectively.
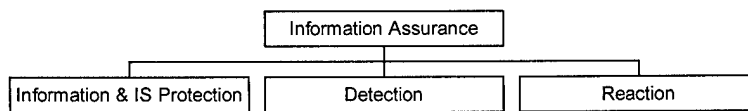
Figure 2-12: Top Tier of IA Value Hierarchy

Suppose the assessed weight for *protection* was in question—this will be the varied weight. The other weights will change, but must retain their original relative importance. The adjusted weights are determined by the following formulas, described in Kirkwood. [1997:83-84] The weight for protect, w_p, ranges from 0 to 1, or a specified interval of interest.

The adjusted weight for *detect* is then given by

$$w_d = (1 - w_p) \times \left(\frac{w_d^o}{w_d^o + w_r^o} \right)$$

Equation 2-4: Adjusted Weight for Detection

The adjusted weight for *react* is then given by

$$w_r = (1 - w_p) \times \left(\frac{w_r^o}{w_d^o + w_r^o} \right)$$

Equation 2-5: Adjusted Weight for Reaction

2.8. Summary

The documents and topics discussed provide a foundation for understanding some of the relevant Joint- and Service-specific concerns with respect to Information Assurance and the related concept of defensive information operations. Risk management is a process to facilitate the cost-effective implementation of countermeasures to mitigate risks inherent in employing information systems. Other issues concerning the tradeoffs between functionality and security must be addressed when selecting these countermeasures are also emphasized.

The next two chapters will begin by providing an approach to further the focus of the risk management process by constructing a VFT model to quantitatively evaluate the impact of risks based upon the value of the information and information system capabilities. Using this as a basis for identification of countermeasures, a triad of models to address the tradeoffs between *IA*, *Operational Capability*, and *Resource Costs* are developed.

3. *The Value of Information and the Risk Management Process*

"Little minds try to defend everything at once, but sensible people look at the main point only; they parry the worst blows and stand a little hurt if thereby they avoid a greater one. If you try to hold everything, you hold nothing."
Frederick the Great, quoted in Foertsch, *The Art of Modern War*, 26 June 1996
[Joint Publications 3-13, 1998:III-15]

3.1. Introduction

As Frederick the Great noted, it can be self-defeating (if not technically and fiscally impossible) to attempt the elimination of all *known* vulnerabilities. An information system that is invincible against threats such as hackers, viruses, and electromagnetic weapons is likely one that is unplugged and contributes little to the decision making process. As discussed earlier, JP 3-13 requires the information realm to be protected commensurate with the value of the information contained within it. The information itself, particularly its value to decision-makers in making decisions, suggests a starting point to identify what information, information systems, and information processes require assurance, and to what degree that assurance should be provided.

Risk is "something bad that might, or might not, actually come to pass." [Kirkwood, 1997:136] This implies two elements of risk: an undesirable event and the likelihood (or probability) of that event occurring. This chapter discusses the application of value focused thinking (VFT) to provide a method to enhance the risk analysis process by using the value of information as a quantitative proxy—capturing the magnitude of a specified 'undesirable event.' This is a paradigm shift from methods that rely upon general, categorical measures such as *high*, *medium*, and *low*, methodologies that may regard the classification level of information to be only determining element of risk, and methodologies that do not adhere to the principles of measurement theory.

3.2. The Value of Information

What makes information important? There are many attributes of information that may be measured, and many that depend upon the context of the situation and the prior knowledge of the decision-maker.

3.2.1. Role of Information in the Military

Due to the increasing reliance upon information technology and the ubiquitous nature of information in military operations, achieving and sustaining information superiority will enhance all other operations. Figure 3-1 compares the increasing levels of access, speed, and amount of information available to war fighters.
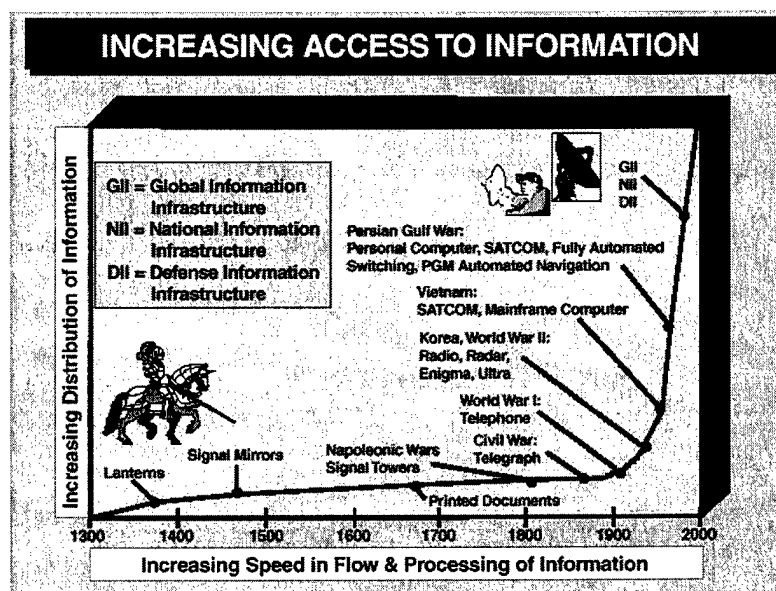

Figure 3-1: Access to Information over Time [JP 3-13, 1998:I-12]

Better information, gathered from large, reliable arrays of sources, processed, and delivered with high fidelity processes and systems, provides an advantage over adversaries by knowing the status of friendly, adversarial and allied forces, and reducing uncertainty in the battlefield.
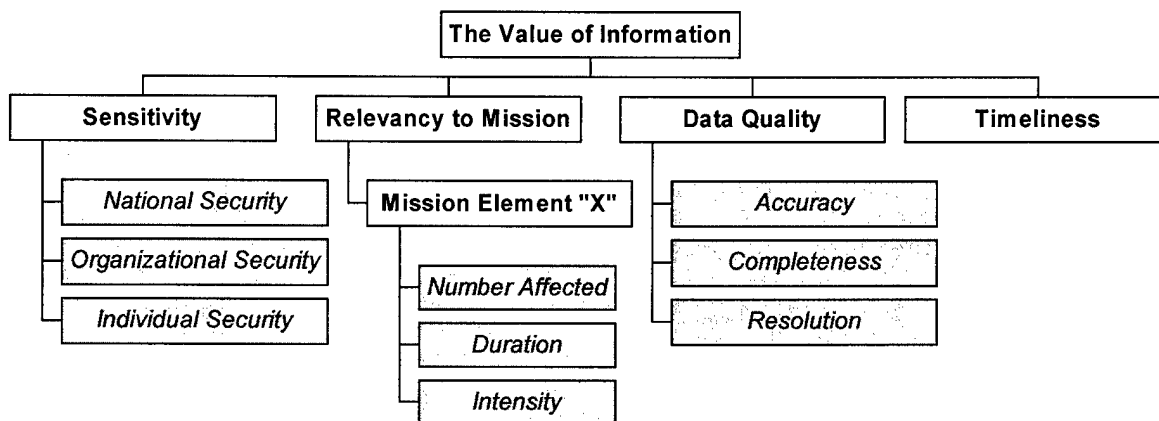
3.2.2. Modeling the Value of Information

Overview

Figure 3-2 illustrates the *Value of Information* value model developed with the help of high-level decision-makers and technical experts. The individuals, assigned to the Air Force Institute of Technology (AFIT), included the designated approval authority (DAA), the director of the communications and information directorate, and the chief of the systems administration branch. During implementation of the entire set of models proposed in this thesis, involvement of individuals with similar levels of authority and expertise will be required. [Kelso, 1999a-b; Maynard, 1999a-b, 2000]

From the elicitations that were accomplished up to this point, it was decided in the target context that the major contributors of value to information were the *sensitivity*, *relevancy*, *data quality*, and *timeliness* of the information itself. [Kelso, 1999a]

```
                        ┌────────────────────────┐
                        │ The Value of Information│
                        └────────────────────────┘
        ┌───────────────────┬──────────────┴────────────┬──────────────────┐
┌───────────────┐ ┌───────────────────┐ ┌───────────────┐ ┌───────────────┐
│  Sensitivity  │ │Relevancy to Mission│ │  Data Quality │ │  Timeliness   │
└───────────────┘ └───────────────────┘ └───────────────┘ └───────────────┘
```

National Security	*Mission Element "X"*	*Accuracy*	
Organizational Security	*Number Affected*	*Completeness*	
Individual Security	*Duration*	*Resolution*	
	Intensity		

Note: The number ("X") of Mission Elements is determined by the Decision Maker

Figure 3-2: Information Value Hierarchy

The purpose of this model is to aid in the risk management process. This process "anticipates needs in all defensive IO and includes planning for both protection and response based on a consideration of information needs, the value of information that may be

compromised or lost if the protected information environment is breached (loss of access control)...." [JP 3-13, 1998:III-7] JP 3-13 further states "the value of information can change from one phase of a military operation to the next and must be considered in risk management." [1998:III-8] From these statements, aspects of information that contribute to the overall value, directly or indirectly, include its sensitivity, its relevancy to a particular mission, its quality, and its timeliness. These four areas relate to four areas of concern expressed by the DM. These included: the compromise of sensitive information, the denial of access to required information (either through destruction of the information itself or blocking the mechanisms of transfer), the unauthorized change of information, and the intentional disruption of information transfer. Based upon the participants' statements and documents addressed, it was assumed that these characteristics composed a mutually exclusive and collectively exhaustive collection that contributed to the value of information. While the model presented here was built on an unclassified system, the principle can be extended to a classified system.

Sensitivity

Ascertaining the value of information may be partially accomplished by examining the risks associated with the unintended compromise of information, accidental or otherwise. The compromise of information has varying consequences; examples include loss of privacy, fraud, loss of life, reduced levels of National Security, inability to maintain Information Superiority or any combination of these items. Figure 3-3 summarizes survey results of estimated financial losses due to a variety of computer crimes.

These losses only include those that were reported and could be reasonably estimated, and therefore do not account for losses due to lack of confidence or weakened competitive

advantage. Note that theft of proprietary information and financial fraud, both resulting from a

compromise in sensitive information, account for a large portion of these total losses.

Method	Incidents			Total Losses ($)		
	1997	1998	1999 *	1997	1998	1999 *
Theft of Proprietary Info	21	20	23	20048000	33545000	42496000
Sabotage of Data/Networks	14	25	27	4285850	2142000	4421000
Telecom Eavesdropping	8	10	10	1181000	562000	765000
System Penetration by Outsider	22	19	28	2911700	1637000	2885000
Insider Abuse of Net Access	55	67	81	1006750	3720000	7576000
Financial Fraud	26	29	27	24892000	11239000	39706000
Denial of Service	n/a	36	28	n/a	2787000	3255000
Spoofing	4	n/a	n/a	512000	n/a	n/a
Virus	165	143	116	12498150	7874000	5274000
Unauthorized Insider Access	22	18	25	3991605	50565000	3567000
Telecom Fraud	35	32	29	22660300	17256000	773000
Active Wiretapping	n/a	5	1	n/a	245000	20000
Laptop Theft	160	162	150	6132200	5250000	13038000
Total				$100,119,555	$136,822,000	$123,776,000

Source: Computer Security Institute -- CSI/FBI 1999 Computer Crime and Security Survey (www.gocsi.com/losses.htm)

Figure 3-3: Estimated Financial Losses due to Security Crime

In the context of government and military information, there are several standards of

evaluating the sensitivity of information, and may be divided into *National*, *Organizational*, and

Individual categories. Overall, it is assumed that more harmful consequences of compromise

imply a higher level of value inherent within the information.

Sensitivity (To National Security)

Classified national security information requires protection against unauthorized

disclosure. [President, 1995:3] The level of classification is dependent upon the damage to the

"national security [harm to the national defense or foreign relations of the United States] from

the unauthorized disclosure of information, to include the sensitivity, value, and utility of that

information." [President, 1995:4] The security classification guidance provides a process to

assess, in detail, the resulting loss or adverse impact to National Security if a specific item of

information is compromised. Therefore, the information's classification level is used as a proxy

to evaluate the information's sensitivity to National Security issues. Figure 3-4 illustrates the evaluation function elicited from the decision-makers.

Sensitivity (National Security)
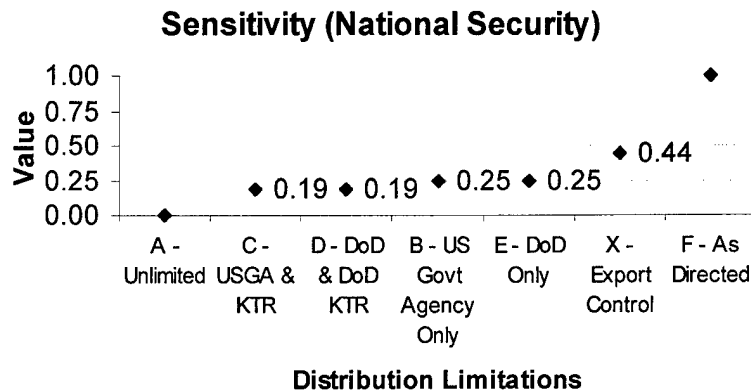
Figure 3-4: Value Function (VF) for Sensitivity (National Security)

Note that all categories, for the test site, are levels of unclassifed information, due to system-specific requirements. These levels were based upon categories specified in DoD Directive 5230.24, which governs distribution limitations based upon the type of information involved. The evaluation measure may be changed to accommodate systems employing classified information. An example of such a scale is shown in Table 3-1.

Table 3-1: Levels of Classification [DODD 5200.28, 1988:27]

Potential Evaluation Categories for Systems with Classified Information
Unclassified
Not Classified but Sensitive (Sensitive in the context that is applicable to National Security)
Confidential; Confidential with one or more categories
Secret; Secret with one or more Special Access Program (SAP) requirements
Top Secret; Top Secret with one or more SAP requirements

Sensitivity (To Organizational Security)

The operations security (OPSEC) process allows the identification of critical information at the organizational level. This process identifies information pertaining to "friendly actions attendant to military operations and other activities." [JP 1-02, 1999:328] For this evaluation

measure, five categories of potentially sensitive information that would afford an adversary an advantage against the organization (AFIT) were determined. It is assumed that the greater the advantage presented the higher the level of value of the information. These categories, ranked in order of importance to the DM, included administrative, financial, virtual infrastructure (i.e. information systems connectivity), physical infrastructure, and personnel activity information. The evaluation function is shown in Figure 3-5. Although it was felt that this set of categories was collectively exhaustive and mutually exclusive for the sample organization, other organization-specific categories should be developed as necessary.
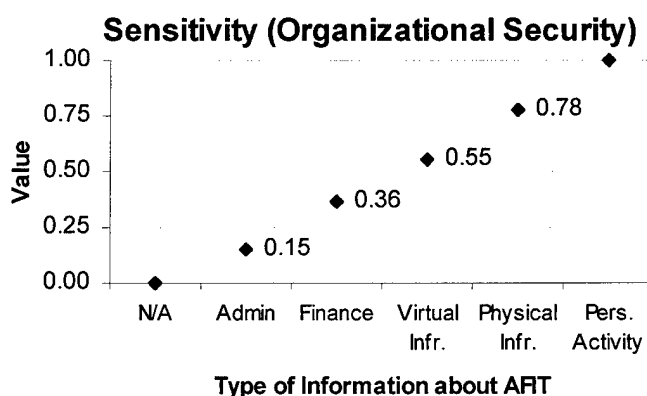
Figure 3-5: VF for Sensitivity (Organizational)

Sensitivity (To Individual Security)

The last evaluation measure for sensitivity focuses on assessing the value of information pertaining to individuals within the organization of interest. This was accomplished by using current legislature or guidelines (e.g. The Privacy Act of 1974). The Privacy Act of 1974 governs the control of certain facts about individuals, implying that inadvertent or careless release may prove harmful due to fraud, loss of privacy, or other individual concerns. Personal information governed by this act is assumed to have more value than personal information not directly covered in the legislation.

Sensitivity (Individual Security)
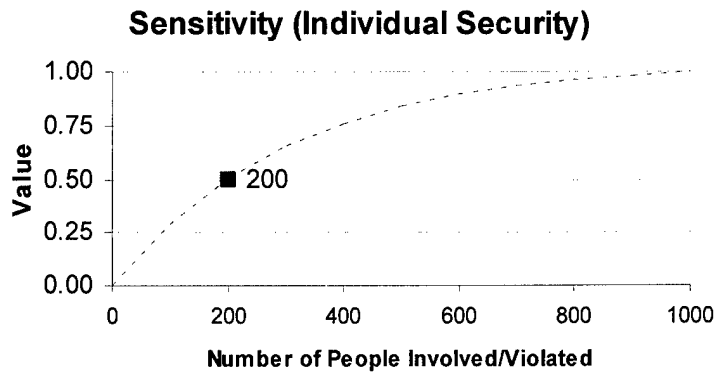
Figure 3-6: VF for Sensitivity (Individual)

The ranges were based upon the number of people, on average, permanently assigned to

AFIT. The scale represents the number of people that would be affected if sensitive individual

information were compromised. This differentiates between compromises of a single or a few

individuals and databases containing sensitive individual information. A mid-value of 200

people was elicited, and resulted in the evaluation function shown in Figure 3-6.

Relevancy to Mission

The relevancy of information pertains to how important the information is to

accomplishing the mission. For this objective, the DM must first identify the mission elements

they most value, hence the "Mission X" notation seen in the hierarchy Figure 3-2. Once these

mission elements are identified, an evaluation of the tradeoffs between them is accomplished

through elicitation of weights. Using the organizational mission statement and DM preferences,

three mission elements were originally evaluated for AFIT. However, the general process is

described only once for brevity.

It is assumed that highly valued information required for mission accomplishment that is

denied to the decision-maker (either by denying access or destroying it altogether) will have a

potentially greater impact upon mission effectiveness than information that is less valued.

Concerns that further establish the relevancy of information to an organization's mission include:

- The number of personnel or organizations affected;
- How long the information can be unavailable before adverse effects upon mission accomplishment are perceived; and,
- The intensity upon which the completion of the mission relies upon the information

Relevance (Number Affected)

The first concern is the number of personnel or organizations affected. This serves as a

proxy for the magnitude of the effects (internal to the organization) that may occur if information

is lost (i.e. deleted or corrupted beyond use) or access to data and/or the system is denied. For

each mission element, a target population is defined, based upon their level of support for that

element. This provides a method to further discriminate information of interest, and provides a

baseline for the percentage that is assessed. Figure 3-7 shows the value function. An

exponentially increasing curve, with a mid-value point at 10% of the population was elicited.
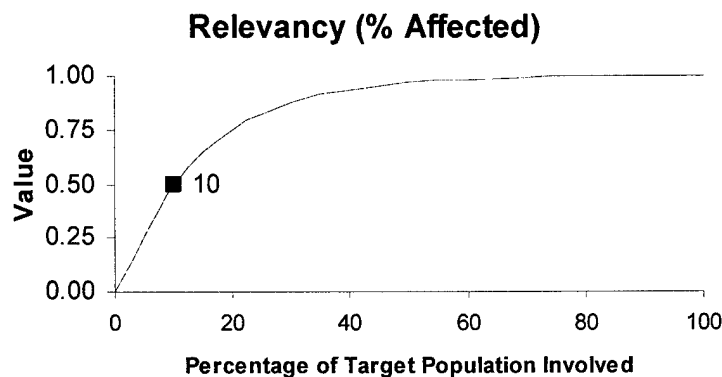

Figure 3-7: VF for Relevancy (Number Affected)

Note that although the percentage may be difficult to estimate, the same measure could

be applied to any organization.

Relevance (Duration)

The second concern in *relevance to mission* is how long the information can remain

unavailable before adverse effects upon mission accomplishment are perceived. Given that the

information is relevant to mission accomplishment to some extent, it is assumed that the more

often the information is required for decision-making processes, the more valuable it is compared

with similar categories of information. The evaluation function, shown in Figure 3-8, shows an

exponentially decreasing curve with a mid-value point at 2 days. It was assumed that

information infrequently used (i.e. once every 14 days or more) was of little value, compared to

information required on a daily (or hourly) basis.

If a system contained critical data that was infrequently accessed, but essential when

required, this measure would require revision. Again, for the test case, it captured the decision-

maker's preferences.

Relevancy (Duration)
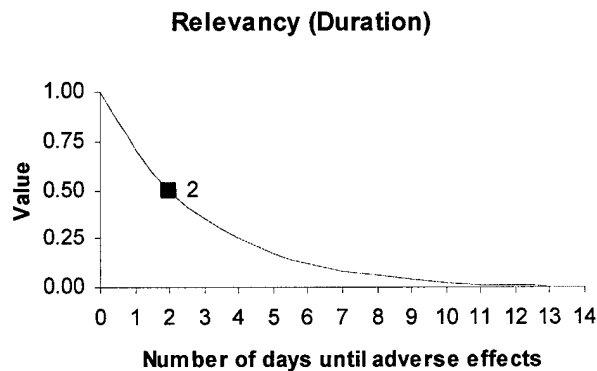
Figure 3-8: VF for Relevancy (Duration)

A similar concept to this approach, the *accessibility factor*, is discussed in the

information technology security (ITSEC) concept of system classes used in the Defense

Information Technology Security Certification and Accreditation Program (DITSCAP). These

classes facilitate the determination of minimum-security requirements for an entire system, based

upon a profile of its characteristics. The categories for this factor, shown in Table 3-2, could be used as an alternative evaluation measure, albeit it is somewhat vague.

Table 3-2: Accessibility Factor Categories [DOD 5200.40-M (Draft), 1999:AP2-5]

Accessibility Factor: The degree that the operation, data, infrastructure, or system needs to be available from a security perspective.	
Reasonable	The specific aspect must be available in reasonable time to avoid operational impacts.
Soon	The specific aspect must be available soon (timely response) to avoid operational impacts.
ASAP	The specific aspect must be available as soon as possible (quick response) to avoid operational impacts.
Immediate	The specific aspect must be available immediately (on demand) to avoid operational impacts.

Relevancy (Intensity)

The third concern regarding the relevancy of information to mission accomplishment is denoted by *Intensity*. This provides subjective assessment of the role information plays in the reduction of uncertainty. Three categories were developed—Preferred, Mission Essential, and Mission Critical—and the elicited value function is shown in Figure 3-9.
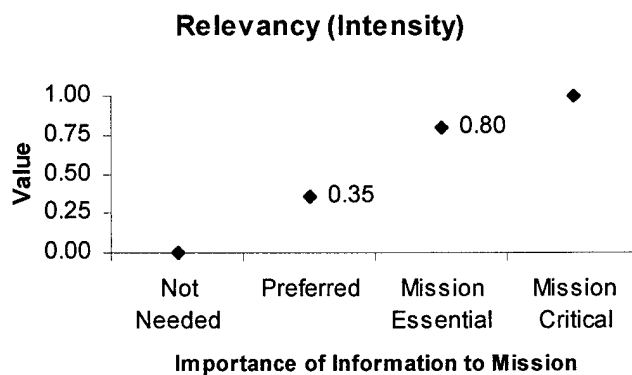
Figure 3-9: VF for Relevancy (Intensity)

Once again, a similar concept is seen in the DITSCAP guidance, denoted as the *mission reliance factor*, and is described in Table 3-3.

3-11

Table 3-3: Accessibility Factor Categories [DOD 5200.40-M (Draft), 1999:AP2-5]

Mission Reliance Factor: The degree that the success of the mission relies on the operation, data, infrastructure, or system.	
None	The mission is not dependent on the specific aspect.
Cursory	The mission is dependent on the specific aspect.
Partial	The mission is partially dependent on the specific aspect.
Total	The mission is totally dependent on the specific aspect.

In summary, if information is relevant to the mission it is valuable. Relevant information that applies to a larger proportion of the organization than otherwise is more valuable. Relevant information that decision makers can only go short periods without adverse affects upon mission accomplishment is more valuable. Finally, relevant information that is relied upon for specific purposes to accomplish the mission is even more valuable. It is also important to note that not only the mission elements, but also the ranges used for each evaluation measure scale, can be modified in order to accommodate organization-specific situations.

Data Quality

Technological advancements allow today's organizations to create, store, and process tremendous amounts of data. As organizations increasingly rely upon this data, "it is obvious that poor data quality may negatively affect organizational effectiveness and efficiency." [Abate, Diegert, and Allen, 1998:1] The United States Army Field Manual (USA FM) 100-6, entitled *Information Operations*, cautions that sources of information are imperfect and susceptible to distortion and deception, requiring commanders and planners to carefully assess the quality of the information before its use. The following six criteria are recommended.

- *Accuracy.* Information that conveys the true situation.
- *Relevance.* Information that applies to the mission, task, or situation at hand.
- *Timeliness.* Information that is available in time to make decisions.
- *Usability.* Information that is in common and in easily understood formats and displays.
- *Completeness.* All necessary information required by the decision-maker.
- *Precision.* Information that has the required level of detail. [USA FM 100-6, 1996]

US Army doctrine takes a further step and prioritizes these characteristics of data quality. As a first priority, information should be accurate and relevant. Second, it should be both timely and in usable form. Finally, information should be as complete and precise as possible. The following rules of thumb supports these relationships: "incomplete or imprecise information *is better than none at all*; untimely or unusable information *is the same as none at all;* inaccurate or irrelevant information *is worse than none at all.*" [USA FM 100-6, 1996] It should be noted, however, that if the imprecise information is the result of enemy deception efforts, no information might be preferred.

Of the six characteristics, relevance has been discussed. Decision-maker involvement concluded that *timeliness* was a value separate from *data quality*, and is discussed in the next section. Usability, within the context presented in FM 100-6, is assumed a function of the information system and the human-machine interfaces, both of which are beyond the scope of the model for evaluating information (although it will be considered in the *Operational Capability* value model discussed in Chapter 4). The last three, *accuracy, completeness*, and *precision* were incorporated into the value model in support of *Data Quality*.

Data Quality (Accuracy)

Abate, et. al, define the requirement for *Accuracy* as "the information must be correct, reliable, and certified free of error." [1998:4] USA FM 100-6 defines "information that conveys the true situation" as accurate. To ascertain the importance of information with respect to accuracy, an indirect assessment of the information's tolerance to error is developed.

Information that can withstand large amounts of error and still positively contribute to the decision making process is assumed to be less valuable (in the eventual context of protecting it). This may be due to the decision context or the specific use of the information. However,

information that can only tolerate very small amounts of inaccuracy before becoming useless to the DM is assumed to be more valuable (and will require more protection). The evaluation function developed is an exponentially decreasing curve, with a mid-value point at 10% minimum acceptable error. Based on this reasoning, information that can only withstand small amounts of error is more valuable. Information that can withstand up to 50% error essentially may contribute more uncertainty into decision-making, and is therefore of little value.

Data Quality (Accuracy)
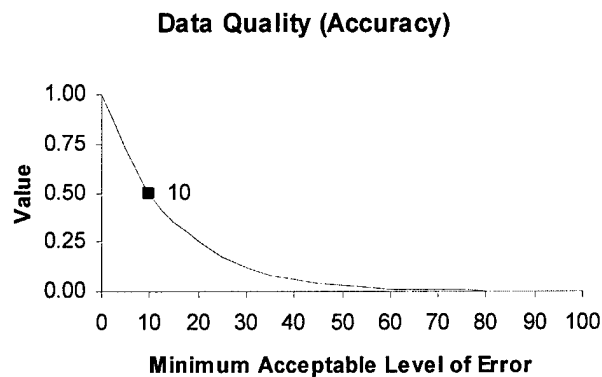
Figure 3-10: VF for Data Quality (Accuracy)

Data Quality (Completeness)

Completeness may be described as "sufficient breadth, depth, and scope for the task at hand." [Abate, et. al., 1998:4] Using a similar approach to the *accuracy* measure, the maximum percent of degradation allowed before the information can no longer be incorporated into the decision making process is assessed. This suggests a level of robustness. If the information can only withstand small amounts of missing data before it becomes useless, then it is assumed it will require more protection, and is therefore more valuable. Figure 3-11 shows the value function, and a mid-value point of 10% was elicited from the decision-maker.

Data Quality (Completeness)
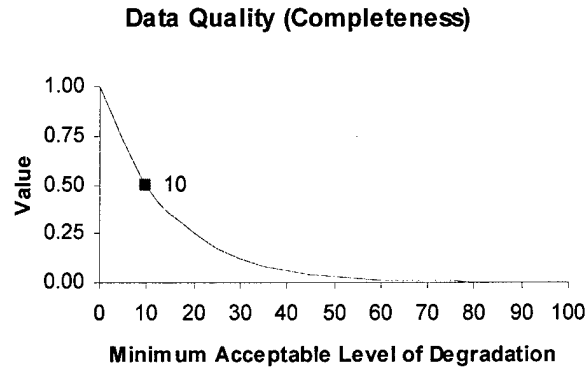
Figure 3-11: VF for Data Quality (Completeness)

Data Quality (Precision (referred to as Resolution))

To ensure that the intent of the model was correctly communicated, the Army's concept of *precision*, "information that has the right level of detail," was restated as *resolution*. This further differentiated this definition from that of accuracy. It was assumed that the higher the level of detail within the information, the more, potential value the information could provide to the DM. It is also important to note that higher levels of detail offer adversaries more opportunity to affect the integrity and remain unobserved, implying the need for more protection.

Data Quality (Resolution)
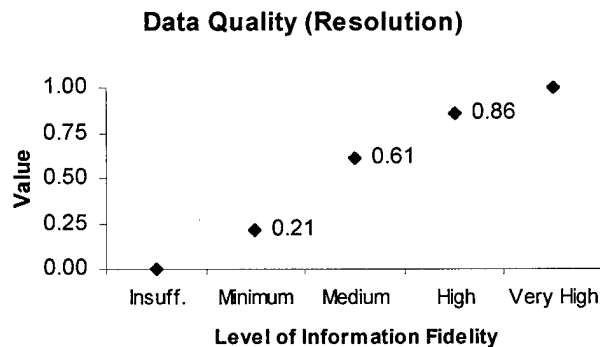
Figure 3-12: VF for Data Quality (Resolution)

Due to the many different types of information, four categories were developed to generalize the level of detail that may be incorporated within information.

3-15

Timeliness

To compound the problem of ascertaining the value of information, one must also
consider the time dynamics of some types of information and how quickly it becomes outdated
and of limited use. The rate of change in value over time is information dependent. Doyle
remarked "the age is best related to the potential cycles of change for a given [piece of
information]. For example, landforms change on a geologic time scale, city infrastructure
changes on a scale of decades, and the position of a targeted aircraft change on the scale of
minutes." [Doyle, 1998:D-7]

Considering that "the age of the data must be appropriate for the task at hand," the rate of
change was used as the evaluation measure. [Abate, et. al., 1998:4] If the information changed
more frequently, then it is implied to have more value than information that is changed less
frequently. Using this generalized concept, appropriate cycle times were developed and
assessed, resulting in the value function shown in Figure 3-13.
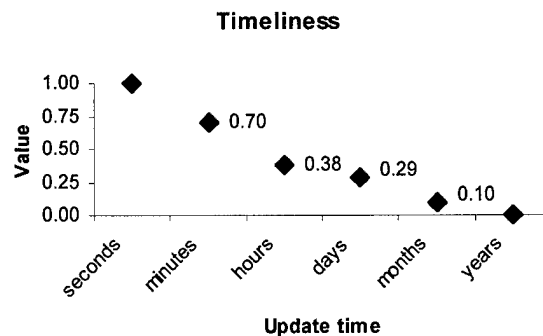
Timeliness

Figure 3-13: VF for Timeliness

If, for some reason, the information flow is disrupted, dynamic information will become
outdated (and of little use) faster; therefore, this information is of high value in the context that it
will require more protection against disruption. Conversely, if the information is static, changing
only frequently, then older data will still be appropriate for decision-making; therefore, this

information has a lower value in the context that it requires less protection against disruptions influencing its timeliness. While these concepts may be generalized, this measure should be revisited for specific organizations.

Weights

Figure 3-14 illustrates the local weight for each objective and evaluation measure.
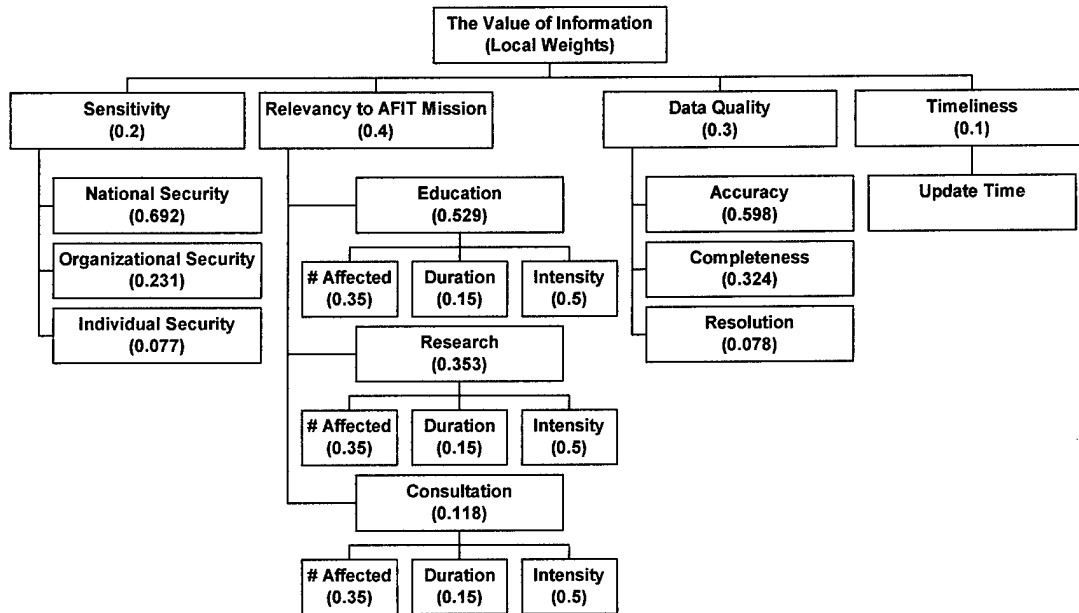
Figure 3-14: Weights Elicited for Value of Information Model

Swing weighting was used to develop these weights. [Kirkwood, 1997:53] Although these weights are organization-specific, the concept must be applied to the remaining three models.

Summary

Threats to information may be defined as "any circumstance or event with the potential to harm an information system (IS) [or the information within] through unauthorized access, destruction, disclosure, modification of data, and/or denial of service." [NSTISSI 4009, 1999:45] Therefore, the risk analysis process should use the value of information as an input to

facilitate the prioritization of assessed risks, and subsequently the prioritization of countermeasures to mitigate those risks.

3.2.3. Risk Management Process

A *risk assessment* is the "process of analyzing threats to and vulnerabilities of an IS and the potential impact the loss of information or capabilities of a system would have on National Security." [NSTISSI 4009, 1999:39] The *risk management process* essentially takes the results of the risk assessment, identifies shortfalls and matches appropriate countermeasures in an economical fashion. [NSTISSI 4009, 1999:39]

To develop effective alternatives for IA strategies, a risk assessment must first be accomplished to establish a baseline of current performance and determine where inadequacies exist. Potential impacts may be evaluated differently for civilian or commercial entities (e.g. profit, or stockholder confidence). However, the *Value of Information* model was built to support both types of organization's information.

The steps of risk assessment include:

- Identify the threat
- Identify the threat likelihood
- Determine the type of attack or attack mechanism
- Determine the vulnerabilities to such attacks
- Identify the immediate and long-term consequences. [IA for Auditors & Evaluators, 1998]

Threat Identification

Although a variety of threats to information and information systems exists, they may be categorized into two areas, natural and human, as shown in Figure 3-15. Natural threats include adverse weather or other acts of God that may destroy, disrupt, deny or alter information or information systems.
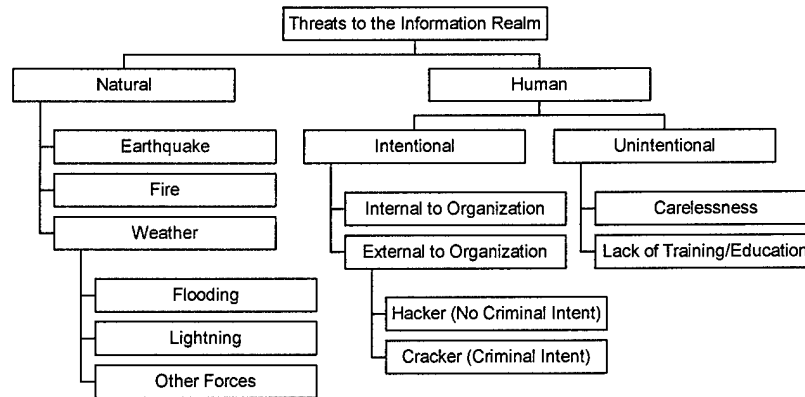
Figure 3-15: Threats to Information [IA for Auditors & Evaluators, 1998]

Human threats are typically identified to be either internal or external to the organization. Among these categories, both unintentional and intentional threats may exist. Unintentional threats may range from fluid spills to poor password choice. Intentional threats, the primary focus of security efforts, are deliberate attacks upon an information system and/or the information that resides within it. [IA for Auditors & Evaluators, 1998]

For the purposes of this thesis, while not discounting the importance of natural occurrences, the threats considered are "intentional acts of attempting to bypass one or more of the following security controls of an IS: non-repudiation, authentication, integrity, availability, or confidentiality." [NSTISSI 4009, 1999:3] JP 1-02 defines computer network attack (CNA) as "operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves." [1999:95]

Identification of these threats is accomplished through internal assessments of practices and procedures, as well as intelligence indicators and warnings. If a threat exists for which there is no corresponding vulnerability (dangling threat) or vice versa (dangling vulnerability), then no risk is assumed to exist. [NSTISSI 4009, 1999:15]

Threat Likelihood

The likelihood of the threat is dependent upon two main factors: capability and motive. The Air Force Information Warfare Center (AFIWC), responsible for vulnerability testing of AF information systems, correlates the likelihood of a threat with the capability required to exploit a known vulnerability. For example, four resources categories (shown in Table 3-4) have been defined that signify "the amount of resources or knowledge required to exploit the vulnerability." [Ferdman and DeNyse, (Final Draft) 2000:30] These categories may aid in estimating the likelihood of a threat actually exploiting a specified vulnerability.

Table 3-4: Categories of Resources Required to Exploit Vulnerabilities

Resources Required to Exploit Vulnerabilities	
A	No equipment or specialized training or knowledge required (e.g., Internet access).
B	Easily obtainable equipment and some knowledge or training is required (e.g., state-of-the-are PC equipment, range of IP addresses, basic knowledge of protocols).
C	Expensive equipment but no specialized training or knowledge (e.g., sophisticated workstations, high-speed network access).
D	Expensive equipment and select knowledge or training (e.g., specific network addresses, firewall protection policies, scripts generators).

Attack Mechanisms

The Defense—Information Assurance Red Team (D-IART) Methodology describes, in detail, vulnerability testing for Department of Defense systems. Due to the distribution limitations of this document, the attack taxonomy is merely summarized in Table 3-5. This summary will serve as the attack mechanisms of interest for the remainder of this document.

Table 3-5: Attack Mechanisms [Derived from MITRE, 1999:Appendix A]

Attack Mechanism	Description
Virtual (or Cyber)	The exploitation of vulnerabilities or weaknesses in the electronic connectivity of information systems or the emanations resulting from their operation.
Physical	The exploitation of vulnerabilities or weaknesses allowing physical access to information components or infrastructure supporting the information system (IS).
Interpersonal	The exploitation of training and/or awareness deficiencies of the individuals that operate, maintain or use the IS and the information that resides within it.

As time and technology progress, threat capabilities evolve, developing new means of attack; however, it may be argued that future methods will fall within one of these three general categories.

Unintentional threat mechanisms may include human (input or judgment) error and inadvertent disclosure. These should be considered on a system-specific basis.

Vulnerability Assessment

AFIWC describes three general approaches to vulnerability assessment. These include the algorithmic approach, the "hacker" approach, and the privilege upgrade approach, each with strengths and limitations.

The algorithmic approach involves a methodical and systematic evaluation of "security features, interfaces, and known security vulnerabilities." [Ferdman and DeNyse, (Final Draft) 2000:3] This approach also encompasses a "review of overall security architecture, regulatory compliance, user security awareness, and other factors. This approach results in a list of potential system vulnerabilities as inputs into the risk assessment process. This method is relatively thorough and does not necessarily require exploiting the vulnerabilities; however, it is the most time intensive of the three. [Ferdman and DeNyse, (Final Draft) 2000:3]

The "hacker" approach (also referred to as "tiger team," "red team," or "penetrate and patch" approaches) involves "a free-for-all attempt to penetrate the system and exploit its vulnerabilities." [Ferdman and DeNyse, (Final Draft) 2000:3] This approach focuses on finding vulnerabilities and exploiting them as a "hacker" would be expected to do. Based upon the usually successful results, this approach often provides powerful incentives to decision makers for initiating appropriate patches and remedial measures. However, the unstructured nature and stringent rules of engagement imposed may result in other, potentially serious, vulnerabilities to remain overlooked. [Ferdman and DeNyse, (Final Draft) 2000:3-4]

Finally, the privilege upgrade approach focuses solely on the penetrator's ability to increase their level of privilege, going from a very limited level to the system administrator level. Although this appears to be the most persistent *modus operandi* of hacker penetrations, this approach considers the fewest areas of the information system that are potentially vulnerable. [Ferdman and DeNyse, (Final Draft) 2000:4]

Identification of Consequences

Referring back to the elements of risk—an undesirable event and the likelihood (or probability) of that event occurring—the undesirable event is based upon the value of the information that is either disclosed, denied, lost, corrupted, or delayed. Given that a threat is identified, a related vulnerability exists, and the threat has a mechanism and the motivation to exploit the vulnerability, an estimated probability of such an event can be determined.

The identification of consequences, or the impact due to exploited vulnerabilities, is where the benefits of the *Value of Information* model are realized. If exploitation were to occur, the potential target, or element of information, can be ascertained and evaluated. Assuming the methods to approximate the probabilities are appropriate, the VFT approach to estimate the

impact should provide an accurate prioritization of risks based upon the decision-maker's preferences and the weaknesses of the system. Such an identification can highlight vulnerabilities, suggest courses of action and be used to more effectively focus resources.

Summary

An overview of the risk management process is shown in Figure 3-16. Assessment of the risk associated with an information system is based upon identifying the threat likelihood, the applicable vulnerabilities that the threat could exploit, and the impact upon the system or the overall mission capability if such an event were to occur. The actual risk is denoted by the intersection of these three factors. Using the *Value of Information* model, the prioritization of the system vulnerabilities by their corresponding level of risk may be enhanced. The next logical step is to identify countermeasures (CM) or controls to mitigate these risks.
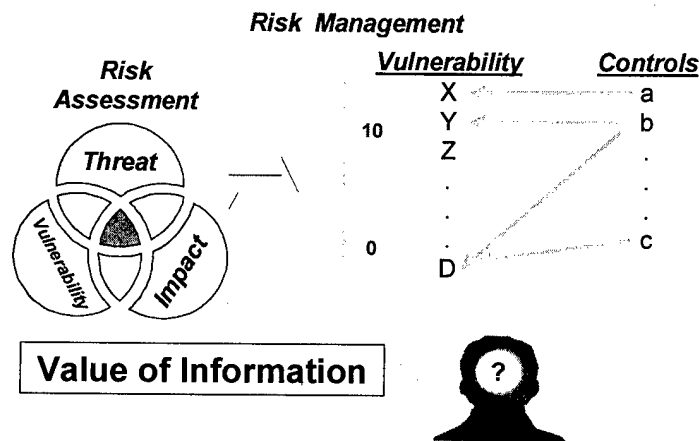
Figure 3-16: Risk Management and the Value of Information Model

However, further tradeoffs must be made between IA, the operational impact upon the system and the costs incurred as a result of CM implementation. The next chapter focuses on the models developed to assist the decision-maker in this endeavor.

4. IA Strategy Evaluation

4.1. Introduction

As discussed earlier, the overall objective of Information Assurance is, like all other major decisions, replete with tradeoffs. The risk accepted by merely operating an information system within today's globally connected information infrastructure, must be balanced with the needs of the organization to accomplish its intended mission, and the costs associated with the information technologies and practices that assure information systems and the information within them.

This initial attempt at modeling these tradeoffs resulted in the construction of three distinct value models, denoted by *IA*, *Operational Capability*, and *Resource Costs*. All of these models are focused on a single decision context—Select the best IA strategy. For the purposes of this analysis, an IA strategy is defined as a collection of technical (hardware, software, and firmware) and non-technical (policies and procedures) means to achieve a desired or improved level of IA. An overview of these models will be presented in this chapter. Specific details are included in Appendix A.

The *IA* model was developed from a combination of 'top down' and 'bottom up' analysis of Joint- and Service-specific doctrine and open literature. Establishing the fundamental objectives was the purpose of the top down analysis. The *IA* model captures the benefits of information assurance. JP 3-13, entitled *Joint Doctrine for Information Operations*, provided many of the definitions and issues associated with Information Assurance for this purpose.

The *Operational Capability* model was developed to provide a better understanding of the enhancements or limitations associated with implementing an IA strategy. In general, more

secure environments are less capable compared to those with unconstrained, unmonitored access.

Values related to operational capability were derived primarily from JP 3-13.

Finally, virtually any IA strategy will incur costs, in either funding, time, or personnel. The *Resource Costs* model was developed to facilitate such cost comparisons between alternatives.
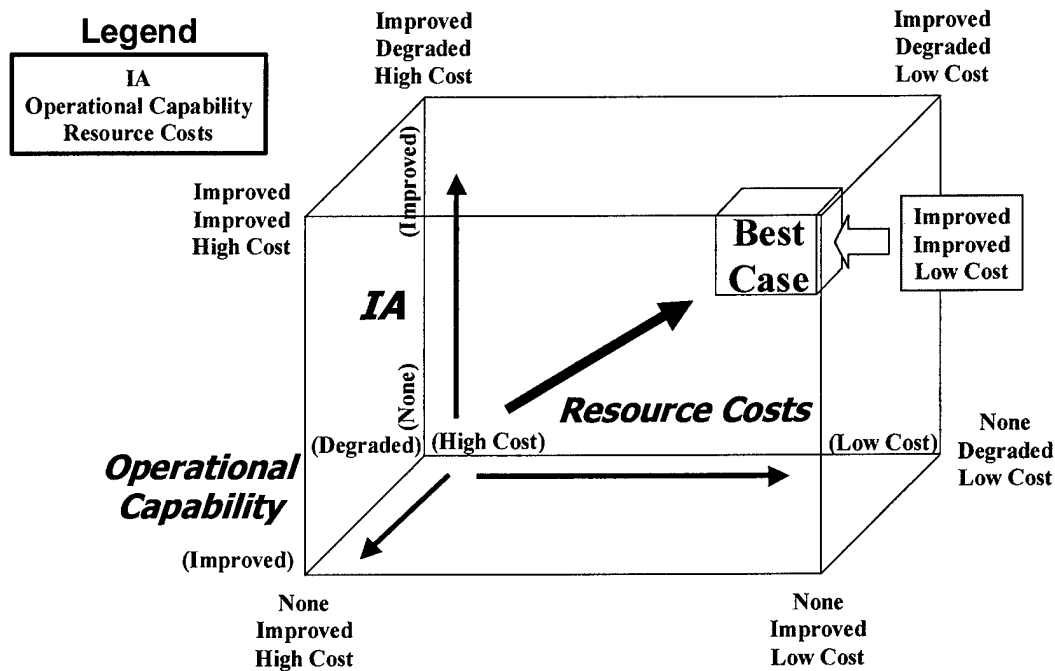
Figure 4-1: The IA Balance

A visual representation of how the three models would be integrated is shown in Figure 4-1. Once a set of IA strategies is evaluated with respect to each model, the decision-maker must then ascertain the tradeoffs between the three axes. This may be accomplished by weighting the results of the three models, and comparing a single number (of overall *value*) from each strategy. Another approach could be to analyze the individual tradeoffs between the hierarchies. The following sections describe the underlying rationale used for model development. A detailed explanation of the value model components is presented in Appendix A.

4.2. Modeling Information Assurance

With the overall goal of achieving Information Assurance in mind, the fundamental

objectives important to this goal must be identified. Using the Joint Doctrine definition of IA

provides the basis for these objectives.

Revisiting this definition,

> Information Assurance "protects and defends information and information
> systems by ensuring their availability, integrity, identification and authentication,
> confidentiality, and non-repudiation. This includes providing for restoration of
> information systems by incorporating protection, detection, and reaction
> capabilities." [JP 3-13, 1998:III-1]
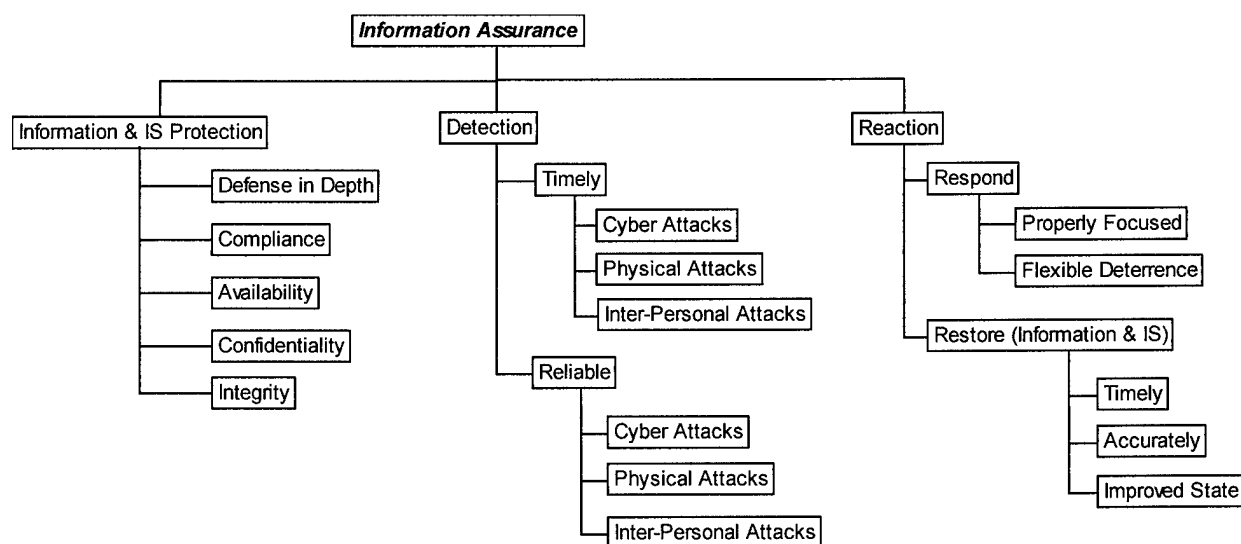
Figure 4-2: IA Value Hierarchy

The stated fundamental objectives of IA are to 'protect and defend information and

information systems.' Defense, however, implies that (1) forces must be aware of an impending

or ongoing attack [detection], and (2) forces have the capability to retaliate in some manner

against the threat [reaction]. From this, the three main values (objectives) that support IA are

derived: *Information and Information System (IS) Protection, Detection,* and *Reaction*

capabilities. Each of these contributes value to the decision-maker by taking part in *assuring* the

intended information and information functions required for *Information Superiority*—"the

degree of dominance in the information domain which permits the conduct of operations without

effective opposition"—or simply day-to-day operations. [JCS IA, 1999:F-12]

It may be argued that taking active measures to detect and react to attacks (thus

mitigating their impact) also support the protection role. In order to clarify these values, and

ensure mutual exclusivity in the value hierarchy, the following definitions used in this analysis

are provided in Table 4-1.

Table 4-1: IA Objective Definitions

IA Objective Definitions
Information and IS Protection: includes those measures taken to afford protection to information and IS, and ensure their availability, confidentiality, and integrity.
Detection: includes measures taken to provide detection of impending or ongoing attacks against an information system or the residing information.
Reaction: includes the measures taken to (1) appropriately respond to an identified attack and (2) restore the information and IS capabilities to an acceptable state, their original state, or an improved state. [Modified from the definition of IA in JP 3-13]

These specific definitions facilitate an independent assessment of each of the IA values,

which are discussed further.

4.2.1. Information and IS Protection

The key elements from the definition (*availability, confidentiality*, and *integrity*) relate to

the desired characteristics of information and information systems in order for them to support

decision-making. Threats to information assurance, and these key characteristics, may be

defined as "any circumstance or event with the potential to harm an information system (IS) [or

the information within] through unauthorized access, destruction, disclosure, modification of

data, and/or denial of service." [NSTISSI 4009, 1999:45] Note that the threats seek to adversely

affect the *availability* (through destruction and denial of service), the *confidentiality* (through

4-4

unauthorized access and disclosure), and the *integrity* (through modification). The motivation, regardless of means, involves the reduction of the information and IS value to the DM. Therefore, measures protecting these characteristics provide value to the decision-maker.

To avoid straying too far from doctrine, other key elements within the definition (*identification and authentication* and *non-repudiation*) should be addressed. From the definition of IA, 'ensuring' these characteristics relates to the means that accomplish the protection of information and information systems. Therefore, the key elements 'identification and authentication' and 'non-repudiation' will be viewed as processes that support the *confidentiality* and *respond* objectives respectively. This is supported simply by the accepted definitions shown in Table 4-2.

Table 4-2: Other Elements of IA

Other Key Elements of IA
Identification: The process an information system uses to recognize an entity. [AFMAN 33-223, 1998:13]
Authentication: A means of identifying individuals and verifying their eligibility to receive specific categories of information. [JP 1-02, 1999:46]
Non-repudiation: Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data. [NSTISSI 4009, 1999:32]

One other value that may be incorporated into information and IS protection is *Defense-in-Depth*. Joint Publication 1-02 defines *defense-in-depth* as "the siting of mutually supporting defense positions designed to absorb and progressively weaken attack, prevent initial observations of the whole position by the enemy, and to allow the commander to maneuver his reserve." [1999:125] This area evaluates the cyber- and physical-hardness of a system, either of which may contribute to protecting one or all of the values *Availability*, *Confidentiality*, and *Integrity*.

The final value contributing to *Information and IS Protection* objective may be termed as *Compliance*, which evaluates the decision-maker's desire to minimize the potential exposure of an information system and its information system to known vulnerabilities. Learning from others' misfortunes is much better than experiencing a similar attack firsthand. Measures that permit the evaluation of this objective account for the efficiency (or lack thereof) by which known vulnerabilities, applicable to the system of interest, are reduced or eliminated altogether.

Table 4-3 summarizes the evaluation measures developed for *protection* portion of the value hierarchy. Each measure is discussed in detail in Appendix A.

Table 4-3: Evaluation Measures Developed for Information and IS Protection

TITLE	MEASURE UNIT	MEASURE TYPE[*]	LOWER BOUND	UPPER BOUND
Defense in Depth				
Time to Penetrate Essential Elements	Ratio: (Time required to attack) / (Time required to defend)	Ratio (S-Curve)	0	4
Physical Security	Probability of Failure	Probability (Exponential)	0	1
Compliance				
Patches Installed	Percentage of applicable patches installed	Percentage (Linear)	0	100
Latency-Implementation	Maximum age of known vulnerability	Months (Linear)	0	6
Latency-Assessment	Time since last vulnerability assessment	Years (Exponential)	0	3
Availability				
Essential Service Uptime	Percentage Availability of Essential Services	Percentage (S-Curve)	90	100
(Overall) System Uptime	Percentage Availability of the Overall System	Percentage (S-Curve)	75	100
Information Redundancy	Number of Data Sources	Quantity	1	4
Confidentiality				
Filter Technology	Filter Type	Category	Packet	Hybrid
Authentication Strength	Identification and Authentication (I&A) Method	Category	None	Combination
Supporting Policy	I&A Support	Category	No-Policy	Policy-Automated
Encryption Strength	Encryption Generation Used	Category	None	State of the Art
Integrity				
Data Integrity	Implementation of Anti-Malicious Code	Category	None	Automated-Full
System Integrity	Percentage of Validated Components	Percentage (Exponential)	0	100
[*] (Shape) of value function, if applicable.				

4.2.2. Detection

"History has shown the value and need for reliable, adequate, and timely intelligence, and the harm that results from its inaccuracies and absence." [JP 3-13, 1998:III-5]

In light of the historical perspective of 'detecting' enemy actions, Joint doctrine also emphasizes, "timely attack detection and reporting are the keys to initiating capability restoration and attack response." [JP 3-13, 1998:III-10] In addition to timely detection, effective defense against IO is "... predicated on how well the intelligence processes function and on the agility of [those involved] to implement protective countermeasures." [JP 3-13, 1998:III-2] This suggests that a certain level of reliability is required to ensure that threats are indeed identified—maximizing the probability of detection and minimizing the probability of false alarms. Additionally, an effective IA strategy must also be robust in that it exhibits timeliness and reliability, regardless of the type of attack (Reference Table 3-5).

As stated earlier, regardless of the type of attack, the earlier an attack (or intrusion) is detected, the quicker an appropriate response can be initiated. Because of the speed at which cyber attacks may be accomplished, timeliness is a vital factor. In addition, due to the nature of available countermeasures, a distinction between internal (or "insider") attacks and external attacks must be made.

The timely detection of physical attacks is dependent upon the level of sophistication of the controls in place as well as the level of awareness of authorized personnel. More sophisticated controls rely less upon human ability to detect an intrusion.

Social Engineering is defined as "a deception technique utilized by hackers to derive information or data about a particular system or operation." [JCS IA, 1999:F-17] There are a number of methods to accomplish this, all of which focus on the lack of awareness or lack of

training that authorized users possess (or both). Timely detection in this context is assumed to rely upon the awareness of the users.

The reliability of intrusion detection systems (IDS) determines how often they fail to detect a valid intrusion, and how often an anomalous event is construed as an intrusion (false alarms). High false alarm rates can consume valuable resources, and could potentially be used to an adversary's advantage. However, failing to detect a valid intrusion is assumed the more serious of the two possibilities.

The detection reliability of physical attacks is assumed to be dependent upon a combination of the organization's physical controls and the level of user awareness. The scope of this model currently appraises those areas under the control of the organization—the information system of interest. However, the connectivity and interdependence of today's systems will eventually require addressing a larger scope, to include the infrastructure supporting the IS. *User Training* evaluates the effectiveness of training programs designed to provide authorized users with the knowledge to recognize (detect) a potential inter-personal attack. Table 4-4 summarizes the evaluation measures developed for the *detection* portion of the value hierarchy.

Table 4-4: Evaluation Measures Developed for Detection

TITLE	MEASURE UNIT	MEASURE TYPE	LOWER BOUND	UPPER BOUND
Timely				
Internal Cyber Attacks	Detection Capability	Category	None	Real-Time (Off Duty)
External Cyber Attacks	Detection Capability	Category	None	Real-Time (Off Duty)
Physical Attacks	Time to Physical Intrusion Detection	Hours (Exponential)	0	72
Interpersonal Attacks	User Awareness	Percentage (Exponential)	0	100
Reliable				
Internal Cyber Attacks	Time Between Configuration	Days (S-Curve)	0	30
External Cyber Attacks	Time Between Configuration	Days (S-Curve)	0	30
Physical Attacks	Control Sophistication	Category	Presence	Automated
Interpersonal Attacks	Training Effectiveness	Category	Not Addressed	Trained & Evaluated

4.2.3. Reaction

Joint doctrine addresses the importance of response and restoration capabilities. [JP 3-13, 1998:III-10] In this analysis, *respond* and *restore* comprise the sub-objectives for *reaction*, since both are dependent upon either attack detection, attack warning, or some other, perhaps natural, event that has caused or has the potential to cause some level of disruption. The overall objective of an effective reaction capability is to provide the organization with a properly focused response mechanism, and to restore the availability, confidentiality and integrity of information and information systems to their original or an improved state.

Respond

The *Properly Focused* objective assesses the ability to correctly identify the individuals involved, the vulnerabilities exploited and the motivation for the attack in order to form the most appropriate response against the attacker (or attackers). This process may be accomplished

4-10

externally or internally, measured by Indicators and Warning (I&W) Notification and ID Accuracy, respectively.

Once an attack is detected and those responsible have been identified, the organization must act to mitigate the risk posed to the organization. *Flexible Deterrence* entails taking the appropriate action at the appropriate time. In this research, the appropriate action is either stopping the attack, or collecting evidence to facilitate legal action, or both. Due to scope and security considerations, more active defensive measures have not been captured. The appropriate time required to act upon threats depends upon the type of attack, the subsequent risks, and the capability of the organization.

Restore

The potentially damaging effects of today's attacks on information and information systems often require that an effective reaction capability also permit their restoration. The reliance upon these systems often requires that this process is accomplished in a *timely* manner, recovers the information as *accurately* as possible, and results in *improvements* to the systems, allowing their protection capability to evolve with the threat capability. Table 4-5 summarizes the evaluation measures developed for the *reaction* portion of the value hierarchy.

Table 4-5: Evaluation Measures Developed for Reaction

TITLE	MEASURE UNIT	MEASURE TYPE	LOWER BOUND	UPPER BOUND
Respond (Properly Focused)				
Indicator and Warning Sources	Number of Sources of Warning	Quantity	0	5
Identification Accuracy	Granularity of Non-repudiation	Category	None	Comprehensive
Respond (Flexible Deterrence)				
Timely Initiation of Deterrent Options	Decision Level Required	Category	Automatic	Higher Level
Stop Attack	Process to Stop Attack	Category	No Capability	Automatic
Collect Evidence	Capability to Collect Evidence	Category	No Capability	System-Benign
Restore Information and IS (Timely)				
Time to Restore Essential Elements	Time Required	Time (Linear)	0	Maximum acceptable time specified by organization
Time to Restore to Fully Operational Capable Level	Time Required	Time (Linear)	0	Maximum acceptable time specified by organization
Restore Information and IS (Accurately)				
Restoration Accuracy	Percentage of Information Recoverable	Percentage (S-Curve)	0	100
Restore Information and IS (Improved State)				
Resource Inventory	Percentage of Components Inventoried	Percentage (S-Curve)	0	100
Improved State	Are procedures in place?	Yes/No	--	--

4.3. Consideration of Operational Capabilities and IA

Increasingly complex information systems are being integrated into traditional warfighting disciplines such as mobility; logistics; and command, control, communications, computers, and intelligence (C4I). Many of these systems are designed and employed with inherent vulnerabilities that are, in many cases, the unavoidable consequences of enhanced functionality, interoperability, efficiency, and convenience to users. [JP 3-13, 1998:I-11]

Functionality, interoperability, efficiency and convenience all add value to the operational capability of an information system. Just as vulnerabilities stem from trying to achieve these values, countermeasures to eliminate them often detract from the information system's value. The *Operational Capability* hierarchy accounts for the changes that may result from IA strategy implementation. This hierarchy attempts to measure these effects, and assumes that the DM wants to minimize any adverse impact upon the existent system at a reasonable level of information assurance.
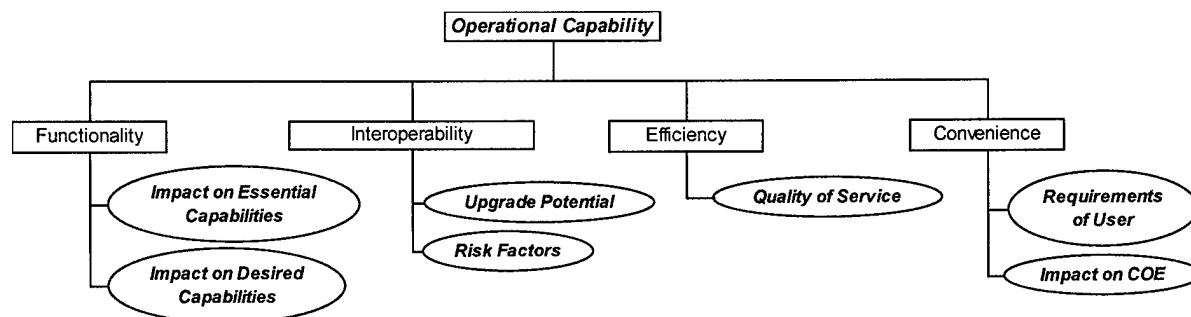
Figure 4-3: Value Hierarchy for Operational Capability

4.3.1. Functionality

Functionality is defined as the usefulness offered to system clients by providing information and information-related capabilities. Attributes that describe the value of the information system regarding functionality are desired and essential capabilities. *Essential* capabilities are those services that an organization currently relies heavily upon to accomplish their stated mission. If these services are no longer made available, it is assumed that other

4-13

means must be found to enable the organization to accomplish mission objectives. *Desired capabilities* are defined as those capabilities that offer enhanced mission effectiveness, but are not required to perform their stated objectives. To ascertain the changes corresponding with an IA strategy, two constructed measures are developed: *Impact on Essential Capabilities* and *Impact on Desired Capabilities*. These assess any impact (good or bad) an IA Strategy may have upon services and information currently accessible to authorized users. This focuses only on those services (or supporting services) that are of value to the DM or the majority of authorized users.

4.3.2. Interoperability

Systems that are interoperable and can be easily integrated with current and future systems provide immediate and cost-effective value to the DM. In the context of ascertaining the value of an IA strategy, *Interoperability* issues are measured with the two attributes *Upgrade Potential* and *Risk Factors*. These measures focus on the potential impact on future maintenance and/or the possibility for upgrades based upon the uniqueness of the components. *Risk Factors* evaluate the additional risk that may be associated with implementation of certain types of countermeasures within a strategy. This risk applies to the likelihood of new vulnerabilities being introduced into the system, to include the possibility of incompatibility. It is assumed that the level of this risk is contingent upon the maturity of the technology, which serves as a constructed proxy for these types of risk.

4.3.3. Efficiency

The efficiency of an information system is dependent upon many factors (e.g. bandwidth, throughput, processing capabilities, routing algorithms, and so forth). Currently, the quality of service (QoS) that an information system provides is predominantly system-specific, based upon

the architecture and operating system employed, and is dependent upon the workload at any given time. Therefore, the degradation of QoS due to the addition of components (countermeasures) may not be perceived consistently throughout the IS, if at all. For these reasons, a categorical assessment of the impact that an IA Strategy may have upon information system's QoS is offered.

4.3.4. Convenience

Convenience relates to the level of complexity involved in the human interfaces designed into the information system of interest. The tradeoffs involved include buying more security at the expense of preventing users from employing the IS and its information in an operationally effective, or timely, manner. Attributes of a system that measure its convenience includes the requirements a user must fulfill in order to gain authorized access, and the demands placed upon the user to employ and benefit from the IS once access is gained. These are captured by *Requirements of User* and *Impact on Common Operating Environment*, respectively.

Table 4-6 summarizes the measures used to evaluate IA strategies with respect to *Operational Capability* considerations.

Table 4-6: Measures Developed for Operational Capability Model

TITLE	MEASURE UNIT	MEASURE TYPE	LOWER BOUND	UPPER BOUND
Functionality				
Impact on Essential Capabilities	Net Change in Essential Services	Quantity (Linear)	-3	3
Impact on Desired Capabilities	Net Change in Desired Services	Quantity (Linear)	-3	3
Interoperability				
Upgrade Potential	Component Source	Category	One-of-a-kind	COTS
Risk Factors	Technology Type	Category	Never been used	Previously used on a similar system with similar configuration
Efficiency				
Quality of Service	Impact on Network Performance	Category	Unacceptable Performance	Improved Performance
Convenience				
Requirements of User	Time to Access System	Time (S-Curve)	0 (seconds)	Maximum acceptable time designated by organization
Impact on Common Operating Environment	Impact based upon previous system	Category	Negative Impact	Positive Impact

4.4. Consideration of the Cost of IA Strategies

"Technology that affects an adversary's information and information systems and protects and defends friendly information and information systems will be pursued at every opportunity to ensure the greatest return on investment." [JP 3-13, 1998:I-5] This statement emphasizes the fact that, in an environment of shrinking budgets, costs associated with implementing an IA strategy must be considered. However, in addition to the acquisition costs, implementation costs must also be taken into account. Figure 4-4 illustrates the cost hierarchy addressed in this research.
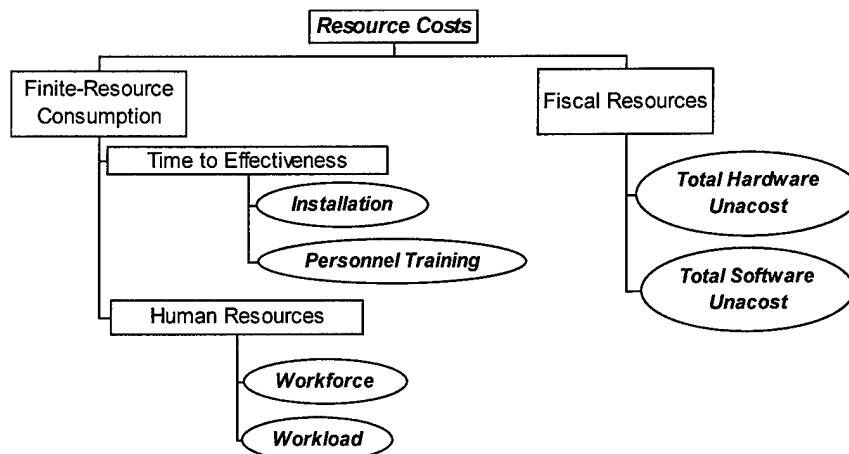
Figure 4-4: Resource Cost Hierarchy

For the purpose of this study, IA costs are grouped into two categories: *Finite-Resource Consumption* and *Fiscal Resources*. *Finite-Resource Consumption* accounts for the tangible, direct costs incurred in time and people that is required to implement an IA strategy. The *Fiscal Resources* accounts for the dollar costs associated with acquiring an IA strategy.

It is important to note that for the evaluation of costs, low-cost alternatives provide more *value* to the DM. Therefore, on a scale from 0 to 10, 0 is least preferred (high cost) and 10 is most preferred (low or no cost). This methodology focuses primarily on the total costs in time,

4-17

people, and money required to procure and implement an IA strategy. Opportunity costs (in dollars), as well as any sunk costs of the legacy system, are not considered. Additionally, salvage value of items being replaced is not directly addressed, but may be incorporated if the appropriate accounting procedures are available. However, the salvage value of IT items is often relatively low.

4.4.1. Finite Resource Consumption

Finite resource consumption captures the amount of time and people required to implement an IA strategy.

Time to Effectiveness

The element of time is important due to the rapid evolution of technology, as well as the threats against it, suggesting that an effective IA strategy is one that can be implemented quickly. The time required in order for a particular countermeasure (CM) within an IA strategy to become effective is a function of two things—how long it takes to install the CM, and how long it takes the appropriate personnel to be trained in the CM. A CM that is easy to install and requires no training for it to be effective incurs less "cost" in time than a CM that is difficult and time consuming to install and also requires significant training time before it becomes operationally effective. The longer a CM takes to implement, the longer the system remains vulnerable. It is assumed that the DM prefers to minimize the time that the organization's information and information system are exposed to vulnerabilities identified.

Human Resources

The personnel element is of importance due to the associated training, management, and overhead costs; however, the real concern is that of technological expertise. High training costs and turnover rates of personnel specializing in information technology and management may

cause an organization to defer an IA strategy requiring more people. [IO Symposium, 1999] The alternative to new workers is requiring overtime of existing personnel. Although, this approach may potentially be cost effective, it is not without consequences and therefore must be considered when evaluating IA strategies.

4.4.2. Fiscal Resources

Recognizing the dollar costs of IA strategies is a key concern, not only with the Defense Department but also with the competitive commercial sector as well, it has been included in the hierarchy. These fiscal costs were broken down into two categories (*hardware* and *software*) to capture DM preferences for each type. *Hardware Costs* include the dollar costs associated with initial procurement, operations and maintenance (O&M), and supporting training dollar costs associated with hardware. *Software Costs* are considered in an identical manner to the *Hardware Costs*.

The assumptions for this evaluation consideration include:

- If salvage costs are known, they are included; otherwise, they are ignored;

- It is assumed that funds are available, and will be procured from the appropriate budget where applicable;

- Any IA strategy under consideration is assumed to be within budgetary constraints throughout its life span; and,

- An alternative that exceeds the organization's budget will not be considered.

To account for potentially varying life spans of the components within an IA strategy, the total discounted uniform annual costs (Unacost) are calculated. This provides a means to facilitate equitable comparisons between the long-term monetary impacts of IA strategies. Unlike using a net present value calculation, this method accounts for variations in useful life, and puts "all systems (IA strategies) on a 1-year basis. Unacost converts any system lasting n

years with a present value P_n to an equivalent 1-year cost as of the end of the year."

[Humphreys, 1983:35] If the DM does not require that the costs be broken down into hardware and software, then all UNACOST values may be added together, while still considering only those strategies that are within the organization's budgetary constraints. Table 4-7 summarizes the measures developed for the *Resource Costs* considerations.

Table 4-7: Measures Developed for Resource Costs Model

TITLE	MEASURE UNIT	MEASURE TYPE	LOWER BOUND	UPPER BOUND
Finite Resource Consumption (Time to Effectiveness)				
Installation Time	Days required to install all components within the strategy	Days (Linear)	0	365
Personnel Training Time	Days required to complete required training associated with strategy.	Days (Linear)	0	365
Finite Resource Consumption (Human Resources)				
Workforce	Percentage change in workforce required	Percentage (Linear)	0	100
Workload	Overtime hours (per week, per person)	Hours (Exponential)	0	20
Fiscal Resources				
Total Hardware UNACOST	Uniform Annual Cost	Dollars (Linear)	0	Determined by applicable budget constraints
Total Software UNACOST	Uniform Annual Cost	Dollars (Linear)	0	Determined by applicable budget constraints

4.5. Illustrative Example

Again, each of the measures and objectives are detailed in Appendix A. However, a notional, illustrative example is offered, demonstrating how the set of models discussed to this point may be used to support the decision-making process.
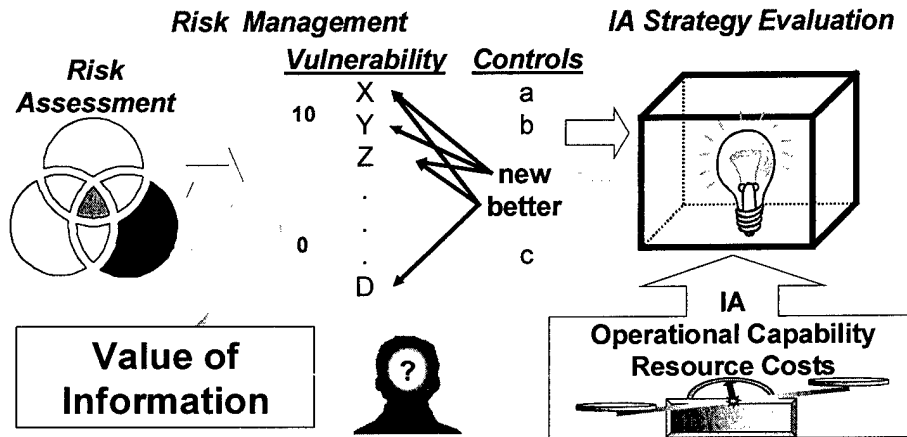
Figure 4-5: IA Strategy Evaluation Process

Figure 4-5 shows the overall process required to implement this methodology. The initial step is to identify system-specific vulnerabilities, and prioritize them by their level of risk, ensuring that this 'risk level' accounts for the value of information that may be adversely affected as a result of exploitation. This process typically identifies a set of controls (technical and non-technical) proposed to mitigate these risks. The set identified may serve as the basis for IA strategy development.

Using the triad of models, the organization must evaluate the levels of performance (for each model) based upon current IA strategies that are already being implemented. This serves two purposes. The first, it establishes a 'baseline' of demonstrated performance, which can be compared to the estimated performance of potential alternatives. Second, this is, in itself, a means to find weaknesses within the current IA strategy of an organization—possibly

4-21

highlighting other areas that the risk assessment may have missed. Areas that score poorly are potential candidates for improvement. New insight may be gained, offering the potential to find new and potentially better controls to construct better IA strategies.

4.5.1. Achieving a Balanced IA Strategy

As seen in Table 4-8, three alternatives are offered: "Do Nothing" (which serves as a baseline), Strategy 1, and Strategy 2. The scales, in this example, are from 0 to 10, signifying the DM preference from least to most preferred respectively. Although the values for all alternatives in the illustrative example were generated in a random fashion, the underlying intentions were to demonstrate potential differences between alternatives, and the considerations (or tradeoffs) that must be made during comparisons.

Table 4-8: Notional Results

Alternative	IA	Operational Capability	Resource Costs
"Do Nothing" (Baseline)	2.3	6.5	2.5
Strategy 1	3.2	7.2	2.6
Strategy 2	5.8	5.0	6.4

Through inspection of the table, both of the proposed strategies will yield some level of improvement in the organization's information assurance. Strategy 1, however, will also provide more operational capability at a slightly less resource cost (note that a score closer to 10 is preferred) than what the organization is currently incurring. Strategy 2 provides a much larger increase in information assurance compared to either Strategy 1 or the *status quo*, and requires fewer resource costs. However, Strategy 2 will result in a decrease in operational capability, compared to what is currently enjoyed by the organization. It should be noted that each proposed strategy might actually be a 'basket' or portfolio of information assurance choices.

The remainder of this section assumes that the *status quo* is an unacceptable option, for one reason or another.

To gain further insight from the evaluation process, the extent to which each strategy contributes to the decision-maker preferences can be analyzed. For example, Figure 4-6 shows the portion of value from each strategy that is attributed to the three main objectives within the *IA* value model. The 'Best Case' at the bottom of the chart shows the weights that would be assigned to each of the objectives. In this example, these correspond to 0.5, 0.3, and 0.2 for *Protection (Information and IS)*, *Detection*, and *Reaction*, respectively.

Information Assurance

Strategy 1 (3.2)
Strategy 2 (5.8)
Best Case (10)

0   2   4   6   8   10

Value

□ Protection □ Detection ■ Reaction
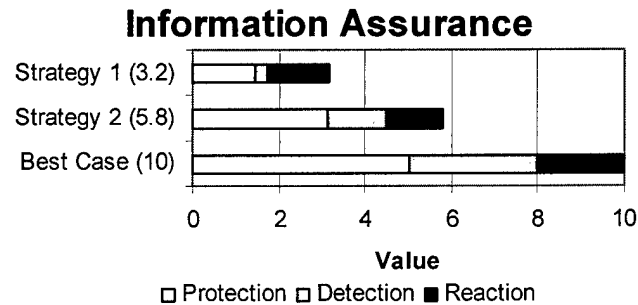
Figure 4-6: IA Results

Again, a similar approach may be taken for the other dimensions of this problem. Figure 4-7 shows which objectives each strategy meets (or more importantly, falls short of) the decision-maker's fundamental objectives within the *Operational Capability* value model.

Operational Capability

Strategy 1 (7.2)
Strategy 2 (5.0)
Best Case (10)

0   2   4   6   8   10

Value

□ Functionality □ Interoperability ▣ Efficiency ■ Convenience
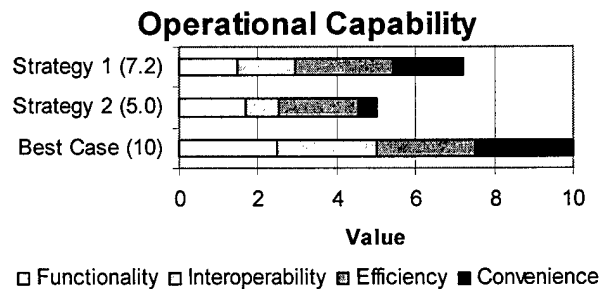
Figure 4-7: Operational Capability Results

4-23

Finally, the same type of graphical analysis is shown for the strategies with respect to the *Resource Costs* value model, shown in Figure 4-8. An added benefit to this type of modeling, as discussed in Chapter 2, is the capability to assess the sensitivity of the results to the underlying assumptions, particularly the weights.

Resource Costs

Strategy 1 (2.6)	
Strategy 2 (6.4)	
Best Case (10)	

0.0   2.0   4.0   6.0   8.0   10.0

Value

□ Time to Effectiveness □ Human Resources ■ Fiscal Resources
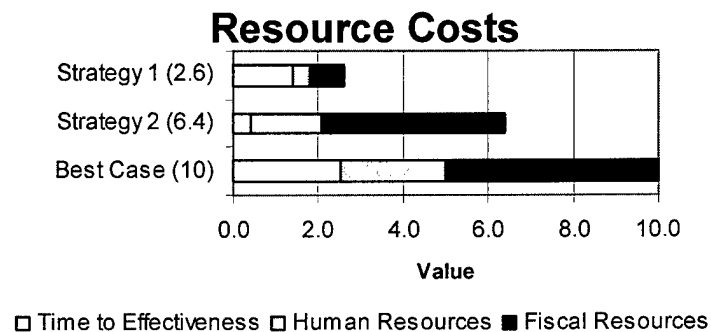
Figure 4-8: Resource Costs Results

According to the 'Best Case' data in Figure 4-8, the current weights are 0.25, 0.25 and 0.5 for the *Time to Effectiveness, Human Resources* and *Fiscal Resources* objectives, respectively. Suppose that the DM noted that Strategy 2 was much more cost effective (*Fiscal Resources*) than Strategy 1; however, evaluation of Strategy 2 revealed that it would take much longer to implement (*Time to Effectiveness*). Unsure about the initial weight assigned to the *Time to Effectiveness* objective, analysis of the sensitivity of the model results to this weight is accomplished, and is shown in Figure 4-9.

Sensitivity Analysis Example
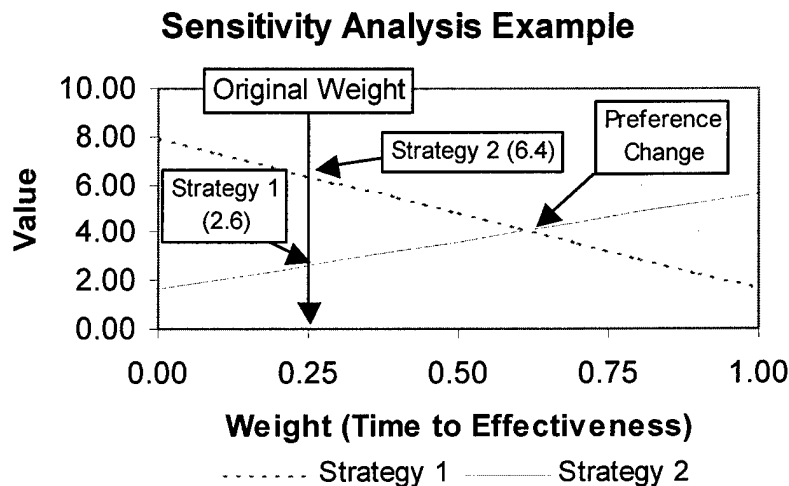
Figure 4-9: Sensitivity Analysis Results

At the point of the original weight for *Time to Effectiveness* (0.25), the values (and subsequently the rank order) of the strategies are shown. However, as the weight for *Time to Effectiveness* is extended beyond (approximately) 0.7, then the preference between the two strategies changes. Note that this only considers changing one weight (within one model) at a time, keeping the relative weighting of all other objectives constant.

Not only do these methods of analysis enable the decision maker to evaluate the tradeoffs between and within IA strategies from a 'big picture' perspective, the results may be broken down to provide information regarding the specific areas where a strategy did (or did not) perform well and why. This further poses a potential for identifying new and improved ways to attain the organization's objectives in each of the three areas.

Figure 4-10 shows a method to graphically compare the subsequent results for all three models simultaneously.

Strategy Evaluation
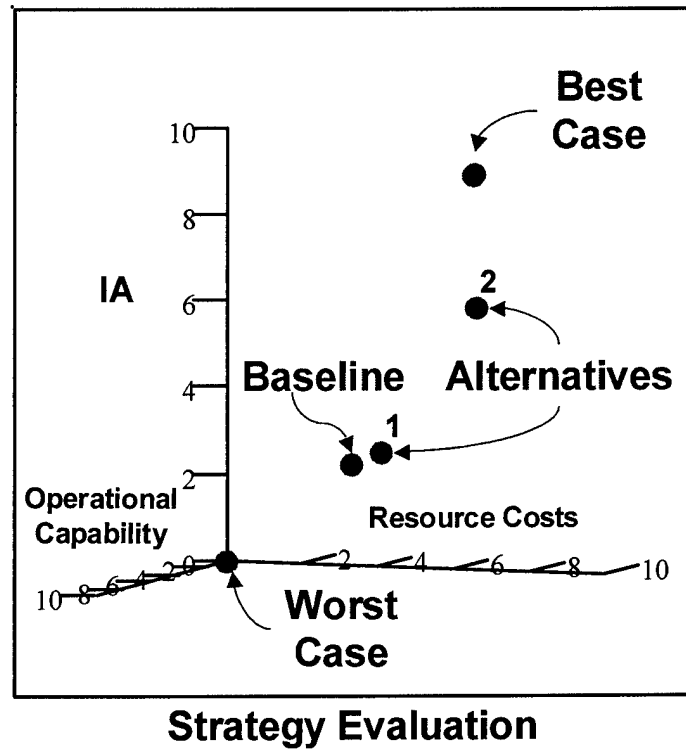
Figure 4-10: Notional Comparison

4.5.2. Summary

The formulation of this analytical framework not only facilitates the evaluation of IA strategies, but the development of them as well. This is accomplished by focusing on what the decision-maker values with respect to information assurance, operational capability, and the limited resources available. This focus quantifies the value added for each component within a strategy, providing a method to balancing the three in order to provide the most overall value to the decision-maker.

5. Findings and Conclusions

5.1. Overview

With the exception of the *value of information* model, no specific decision-maker involvement was directly incorporated into the models described, due to a number of fiscal, time and support constraints. Therefore, these models should be considered a starting point for future analytical efforts to ensure that our country attains a desired level of Information Assurance at a reasonable cost and continuing gains in functionality. In lieu of a detailed analysis of data, Chapter 3 discussed the integration of the value of information into the risk assessment process, a step that should help focus IA efforts. The outputs of this effort, a collection of countermeasures prioritized by their assessed risk, will then lend themselves to evaluation with the triad of value models created to address *Information Assurance, Operational Capability*, and *Resource Cost* considerations.

In light of today's complex information systems, one can only imagine the future applications of information technologies. The incorporation of these models and the value focused thinking technique into the decision-making process for IA is anticipated to reap several benefits.

5.2. Initial Objectives of the Study

A value hierarchy for Information Assurance, derived from the analysis of Joint- and Service-Specific Doctrine was developed. In the process of this work, it was recognized that there were two other major concerns of Joint decision-makers in addition to IA. This necessitated the development of the *Operational Capability* and *Resource Costs* models. All

models present an initial, deterministic, quantification of the values within this context, and are derived from the decision-maker objectives as stated in doctrine.

Further refinement of IA strategy development was gained from the *Value of Information* model, which incorporated preferences and values from the appropriate AFIT decision-makers and information systems experts. With the exception of the *Value of Information* model, limited feedback was received concerning the IA triad of models. This information was favorable, but general in nature. One organization expressed concern over unintended human threats (i.e. an accidental spill on a machine or deletion of a file) and noted that the hierarchy did not appear to address this issue. Although it is recognized that unintentional threats should be considered, the focus of these models was placed upon assuring information and information systems against intentional threats. However, these points further emphasize the need for open communication with decision-makers and technologists in IA-related fields to ensure the incorporation of all appropriate values. Future integration and involvement of these individuals will fill the voids that may exist due to the author's interpretations of doctrine that is intentionally general in nature.

To evaluate alternative IA strategies, measures were developed to assess the level to which these strategies meet (or do not meet) their objectives. This was accomplished mostly through bottom-up analysis, focusing on how current alternatives (countermeasures) differ and why.

The culmination of these efforts resulted in a fully functional decision support tool (developed in Microsoft Excel ©) that enables the decision-makers and system experts to implement the current value models. This tool is capable of accepting inputs for each evaluation measure and the weighting criteria required, as well as providing a summary of results. Minor

5-2

modifications would allow sensitivity analyses and other presentation schema. Additionally, the process required to incorporate new evaluation measures is semi-automated through the use of Visual Basic © macros. All of these aspects facilitate the actual implementation of the described methodology.

5.3. Recommendations for Future Research

First, the value models developed during this study must be reviewed with the appropriate experts in the field. Experts originating from or designated by a sponsor organization that also has an information system of interest is highly suggested. This organization, and their information infrastructure, will serve as a test case to improve upon and validate the proposed measures, and the models they constitute.

Within each of the models, particularly the *Information Assurance* model, several objectives *may* conflict internally within the models, as well as externally between the triad, in some specific settings. Therefore, the sensitivity of these models should be analyzed. Additionally, through the pursuit of a mutually exclusive and collectively exhaustive value hierarchy, mutual preferential independence is assumed. However, this should be verified, once the model has undergone further development and verification. [Reference Kirkwood, 1997:238-240] To aid in such further analysis, a series of prototype hierarchies are presented in Appendix B.

The deterministic nature assumed for this modeling effort may not be entirely appropriate for all circumstances. For example, some controls suggested to mitigate risks are not "100%" solutions. The rapid evolution of not only technology, but the threats against them, also lends the information technology environment to potential uncertainties. The eventual incorporation of utility may prove useful for future decision-makers implementing this model, enabling the

5-3

evaluation of alternatives "in decisions where there is uncertainty about the specific consequence that will result from selecting a particular alternative." [Kirkwood, 1997:245]

Another potential avenue for analytical efforts involves the application of mathematical programming techniques—linear or goal programming, in particular. This assumes that an optimal IA strategy is sought, requiring the maximization of the levels of IA and operational capability while adhering to any applicable resource constraints. One means of approaching this may be accomplished by identifying potential components (technical and non-technical) that comprise the IA strategy alternatives. Once these components are identified, the incremental changes that occur in each of the IA 'triad of models' may be determined, serving as the coefficients within the chosen mathematical model. In order to maintain linearity, interactions between components must either be assumed nonexistent or be grouped to include the entire set. This set is evaluated as either being completely incorporated into the strategy or completely disregarded. Depending upon the possible number of components, this assumption may be ignored in exchange for a potentially very large problem. Existent formulations *of multi-dimensional knapsack* problems with *multiple-choice* constraints and *capital budgeting* problems may provide promising avenues in such an endeavor. [See Murty, 1995:301-305]

It is also important to note that the focus of this research was taken from an organizational perspective. As mentioned in the very first chapter, the connectivity of today's organizations, and their reliance upon each other (particularly within the realm of our Nation's information infrastructures), will eventually require a broader scope. This may be accomplished by either: (1) evaluating systems of systems (an inter-organizational perspective); or, (2) by building upon current policy, facilitating the creation of a common mental model of the elements that are important to everyone concerning Information Assurance.

Despite the level of the perspective, the values considered in the IA problem should remain constant. However, the level of perspective may change the underlying motivations (and therefore the values) concerning the benefits received from a strategy, compared to its impact on capabilities and its cost. A strategy that is regarded as least preferred from an individual organization's viewpoint may be the only acceptable alternative from a National perspective. Fortunately, this is where the strengths of VFT and the set of models will provide common ground to communicate and eliminate weaknesses in our Nation's Information Assurance posture. Nonetheless, this potential area of concern should be considered in future studies.

5.4. Conclusion

There is still much work to be done in this area; the need for Information Assurance will persist as long as information technologies are relied upon. The focus on decision-makers' values will lead to the development of alternatives that have a better chance of fulfilling their IA objectives. Through the proposed set of models, modeling Information Assurance provides a means to accomplish this goal, and a foundation to build upon—offering insight into the difficult and complex problem of Information Assurance.

Appendix A – Value Model Development

Overview

This appendix details the model development using the values and preferences regarding Information Assurance (IA) as derived from Joint- and Service-specific Doctrine, as well as some limited interaction with domain experts. The primary purpose of the IA hierarchy is to evaluate the effectiveness of strategies to enhance the level of information assurance offered to the organization, by assuring its information systems (IS), and the information it handles. These strategies are composed of any number of countermeasures (legacy or proposed), which may consist of technical (hardware, software, and firmware) and non-technical (policies and procedures) means to achieve a desired or improved level of IA. This model incorporates the preferences of the primary decision-maker and stakeholders' interests concerning IA, essentially measuring the costs and benefits due to the strategies implemented.

This methodology assumes the following tasks have been accomplished:

- A vulnerability assessment has been accomplished and results are available;
- Risks have been prioritized based upon their impact and likelihood;
- Countermeasures have been proposed to mitigate the risks identified.

To complement the IA value model, a method to evaluate the "costs," with respect to the resource and operational impacts, of implementing such strategies is also developed. This yielded two additional models—*Operational Capability* and *Resource Costs*—that account for the direct and indirect costs or disadvantages resulting from the implementation of any one or a combination of countermeasures. These models were derived from interviews with SC personnel at AFIT, high-level conferences discussing future IA requirements and open literature on network and information technologies. [Maynard, 2000; IO Symposium, 1999]

The three hierarchies—*IA* (Figure A- 2), *Operational Capability* (Figure A- 3), and

Resource Costs (Figure A- 4)—are then used to perform a tradeoff-analysis, aiding in

determining the strategy that yields the most improvement in IA, the most functionality, at the

least cost. The IA hierarchy is used to determine the marginal level of improvement in the

assurance of a system, whereas the "cost" hierarchies evaluate the total costs incurred by the IA

strategy. The preferred strategy is then determined by evaluating each alternative in the three-

dimensional context shown in Figure A- 1.
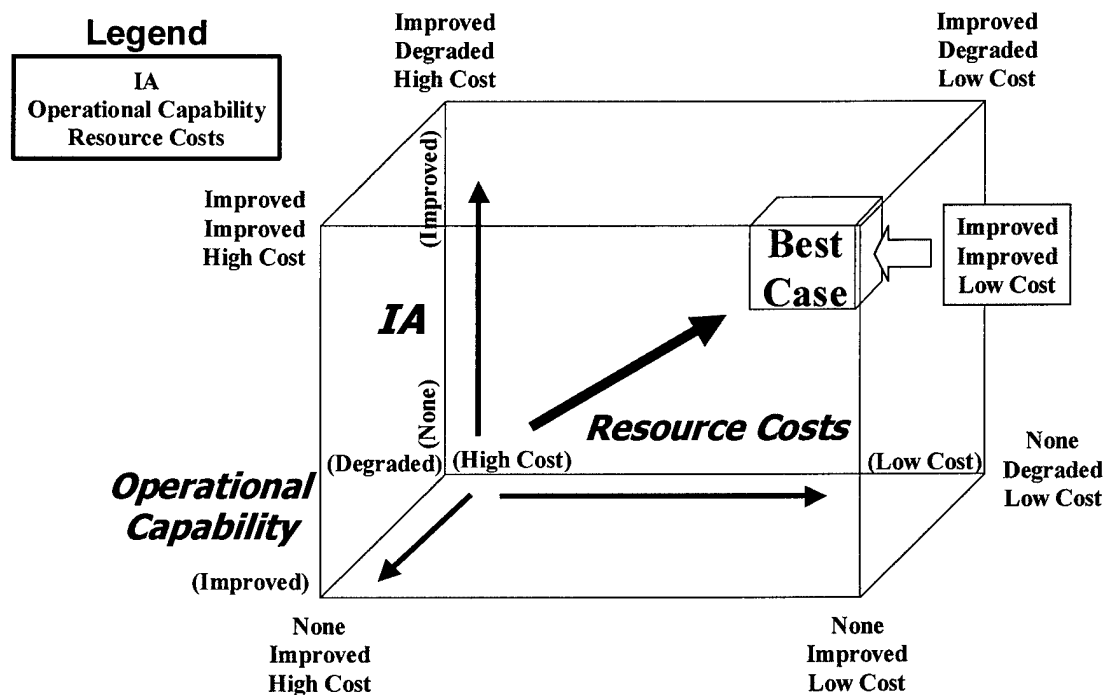
Figure A- 1: Implementation of the Models

Due to time and fiscal constraints, the ranges and values specified within the evaluation

functions are notional, and have not been elicited by a decision-maker. The underlying rationale

for the shapes, however, is discussed when appropriate to highlight the assumptions made about

returns to scale for each measure.

Each of the models is illustrated below for the purpose of familiarizing the reader. A

detailed description of the analysis that yielded theses models follows.
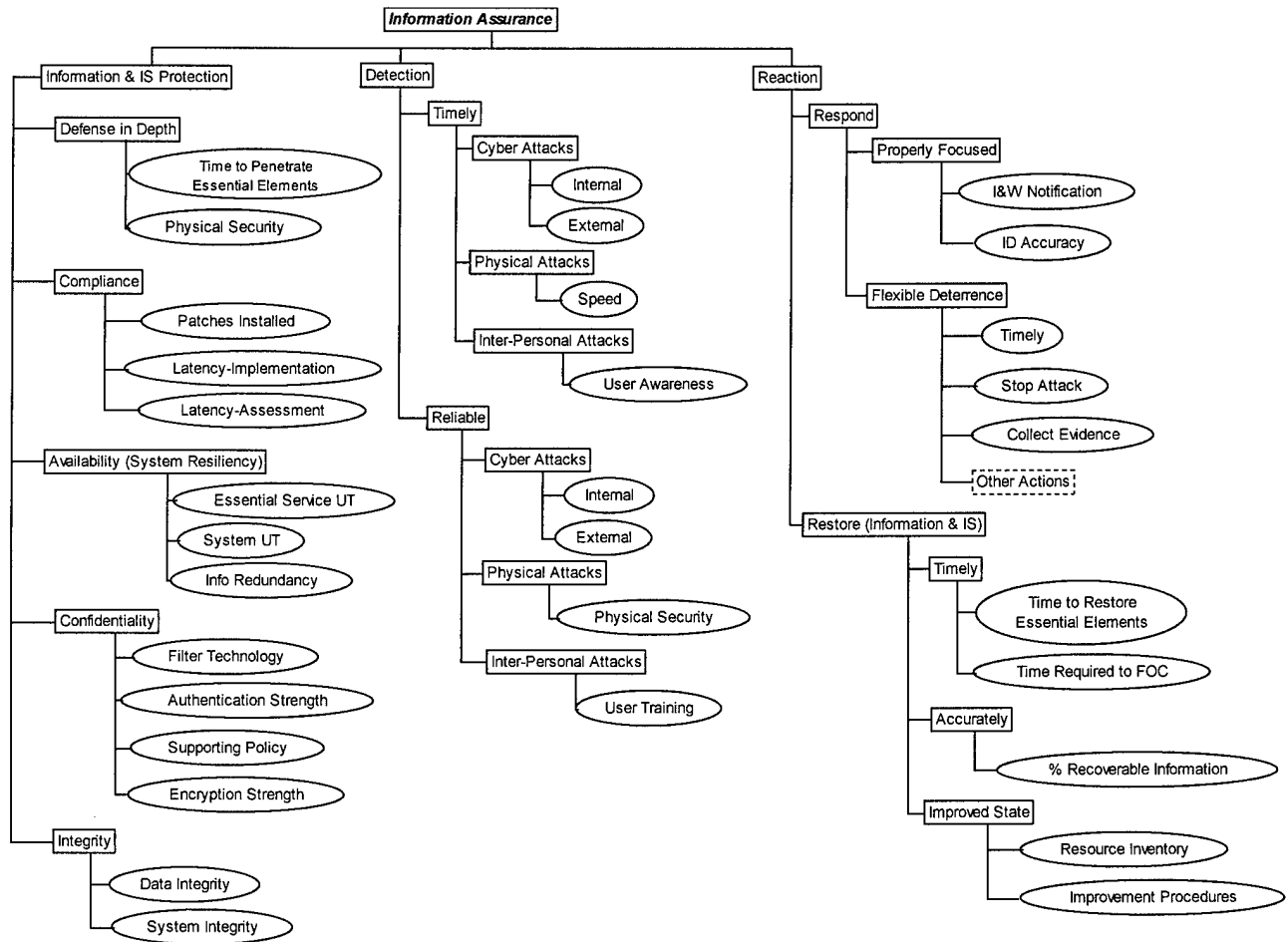
Figure A- 2: IA Value Model
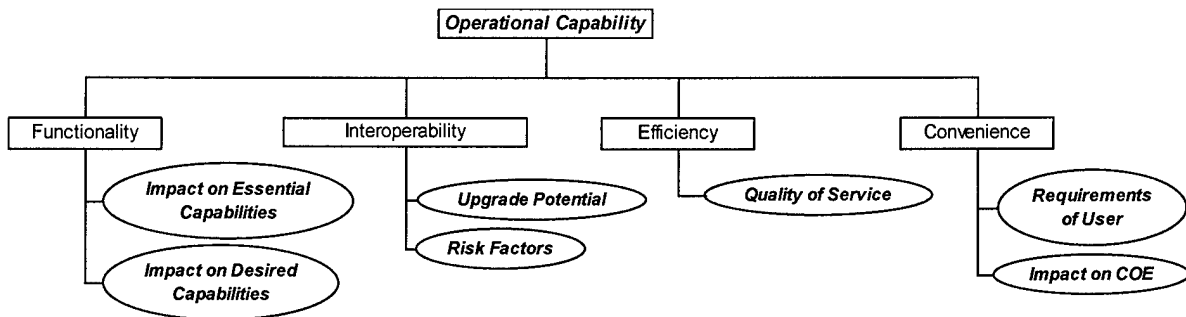
Figure A- 3: Operational Capability Value Model
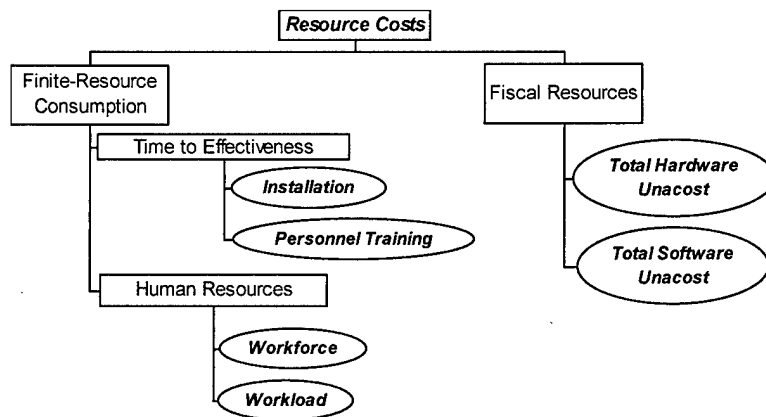
Figure A- 4: Resource Costs Value Model

Scope of Study

Depending upon the perspective, the scope of computer network attack (CNA) varies.

From a computer security perspective, an attack may be defined as "intentional [acts] of

attempting to bypass one or more of the following security controls of an IS: non-repudiation,

authentication, integrity, availability, or confidentiality." [NSTISSI 4009, 1999:3] From a Joint

perspective, CNA is defined as "operations to disrupt, deny, degrade, or destroy information

resident in computers and computer networks, or the computer and networks themselves." [JP 1-

02, 1999:95] Note that the Joint perspective of CNA includes means beyond simply defeating

security controls (e.g. Counterinformation or munitions employment). For the purposes of this

thesis, and the subsequent hierarchies, the scope is limited to the evaluation of attempts

(successful and unsuccessful) to intentionally bypass any security controls managed by the

organization of interest.[1] Assuring information against the other means alluded to in the Joint

definition of CNA, such as Counterinformation Operations and physical destruction of

information systems, are considered beyond the scope of this thesis.

In addition to limiting the types of attacks considered, the types of responses have also

been bounded. In particular, offensive aspects of IA such as information operations (IO) taken

against an adversary are not addressed (e.g. a retaliatory computer network attack against the

source of adversary attacks). On going issues such as legal ramifications, jurisdictional

dilemmas, technical complexities, and potentially classified national capabilities necessitate this

assumption. Actions that facilitate the termination of an attack, the collection of evidence for

legal action, and the restoration of the information and the information systems are included in

this study. It is important to note, however, that Joint Doctrine suggests a strong relationship

between offensive and defensive IO, which suggests that future studies may profit from

including offensive capabilities within an IA strategy to be evaluated.

Information Assurance Value Hierarchy

The IA value hierarchy shown in Figure A- 5 illustrates the areas valued with respect to

IA. The main objectives of information assurance are denoted in the top tier, and are

decomposed further until measures can be derived.

---

[1] The potential for scalability to larger, more complex systems (e.g. the DII) is discussed in Chapter 5.

Information Assurance

- Information & IS Protection
  - Defense in Depth
  - Compliance
  - Availability (System Resiliency)
  - Confidentiality
  - Integrity
- Detection
  - Timely
    - Cyber Attacks
    - Physical Attacks
    - Inter-Personal Attacks
  - Reliable
    - Cyber Attacks
    - Physical Attacks
    - Inter-Personal Attacks
- Reaction
  - Respond
    - Properly Focused
    - Flexible Deterrence
  - Restore (Information & IS)
    - Timely
    - Accurately
    - Improved State

Figure A- 5: Value Hierarchy for Information Assurance

Revisiting the definition of IA,

IA incorporates Information Operations that "… protect and defend information and information systems by ensuring their availability, integrity, identification and authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities." [JP 3-13, 1998:III-1]

The stated objectives of IA are to 'protect and defend information and information systems.' Defense, however, implies that (1) forces must be aware of an impending or ongoing attack [detect], and (2) forces have the capability to retaliate in some manner against the threat [react]. From this, the three main values (objectives) that support IA include *Information and Information System (IS) Protection, Detection,* and *Reaction* capabilities. Each of these contributes value to the decision-maker by *assuring* the intended information and information functions required for *Information Superiority*—"the degree of dominance in the information domain which permits the conduct of operations without effective opposition"—or simply day-to-day operations. [JCS IA, 1999:F-12]

It may be argued that taking active measures to detect and react to attacks (thus mitigating their impact) also support the protection role. In order to clarify these values, and

ensure mutual exclusivity in the value hierarchy, the following definitions used in this analysis are provided in Table A- 1.

Table A- 1: IA Objective Definitions

IA Objective Definitions
Information and IS Protection: includes those measures taken to afford protection to information and IS, and ensure their availability, confidentiality, and integrity.
Detection: includes measures taken to provide detection of impending or ongoing attacks against an information system or the residing information.
Reaction: includes the measures taken to (1) appropriately respond to an identified attack and (2) restore the information and IS capabilities to an acceptable state, their original state, or an improved state. [Modified from the definition of IA in JP 3-13]

These specific definitions facilitate an independent assessment of each of the IA values, which are discussed further in the following sections.

Information and IS Protection

In the context of Defensive Information Operations (DIO), a subset of Information Assurance, the major objective of Joint Force Commanders is to "provide timely, accurate, and relevant information access while denying adversaries the opportunity to exploit friendly information and information systems for their own purposes." [JP 3-13, 1998:I-10] Although JP 3-13 states that IA includes and extends beyond the realm of DIO, this definition essentially provides the characteristics of information and IS that make these items of value to the decision-makers: *Availability* (from timely and relevant), *Confidentiality* (from denying exploitation), and *Integrity* (from accurate). In order to take full advantage of the force multiplying effects of information technologies necessary to achieve information superiority (and possibly avoid total calamity), these characteristics of information and information systems must be protected. Historically, the means of protection have developed into security disciplines such as computer

security (COMPUSEC), information security, emissions security (EMSEC), communications security (COMSEC), and physical security. [AFI 33-202, 1999:3]

Threats to information assurance, and these key characteristics, may be defined as "any circumstance or event with the potential to harm an information system (IS) [or the information within] through unauthorized access, destruction, disclosure, modification of data, and/or denial of service." [NSTISSI 4009, 1999:45] Note that the threats seek to adversely affect the *availability* (through destruction and denial of service), the *confidentiality* (through unauthorized access and disclosure), and the *integrity* (through modification). The motivation, regardless of means, involves the reduction of the information and IS value to the DM. Therefore, measures protecting these characteristics provide value to the decision-maker.

One other value that may be incorporated into information and IS protection are *Defense-in-Depth*. Joint Publication 1-02 defines defense-in-depth as "the siting of mutually supporting defense positions designed to absorb and progressively weaken attack, prevent initial observations of the whole position by the enemy, and to allow the commander to maneuver his reserve." [1999:125] This area evaluates the virtual and physical hardness of a system, either of which may contribute to protecting one or all of the values Availability, Confidentiality, and Integrity.

An additional value may be termed as *Compliance*, which evaluates the decision-maker's desire to minimize the potential exposure of an information system and its information system to known vulnerabilities. Learning from other's misfortunes is much better than experiencing a similar attack firsthand. Measures that permit the evaluation of this objective account for the efficiency (or lack thereof) by which known vulnerabilities, applicable to the system of interest, are reduced or eliminated altogether.

To safeguard that this analysis does not stray too far from doctrine, the other key elements within the definition of IA (specifically Identification, Authentication and Non-repudiation) are viewed as processes that support the *confidentiality* and *properly focused response* objectives respectively. This is supported by the documented definitions shown in Table A- 2.

Table A- 2: Other Elements of IA

Other Key Elements of IA
Identification: The process an information system uses to recognize an entity. [AFMAN 33-223, 1998:13]
Authentication: A means of identifying individuals and verifying their eligibility to receive specific categories of information. [JP 1-02, 1999:46]
Non-repudiation: Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data. [NSTISSI 4009, 1999:32]

Information & IS Protection: Defense in Depth

Increasing the *defense in depth* protects information and information systems by affording the commander more time for attack detection and reaction. It may be argued that assessments of the virtual (i.e. cyberspace) and physical hardness of systems should be accomplished for each of the availability, confidentiality and integrity areas. However, Joint doctrine identifies "defense in depth" as a valuable attribute to information systems concerning risk management as a whole, suggesting incorporation into the model as a separate value. Maximizing the defense in depth commensurate with the value of the elements protected is the objective. Two measures to assess
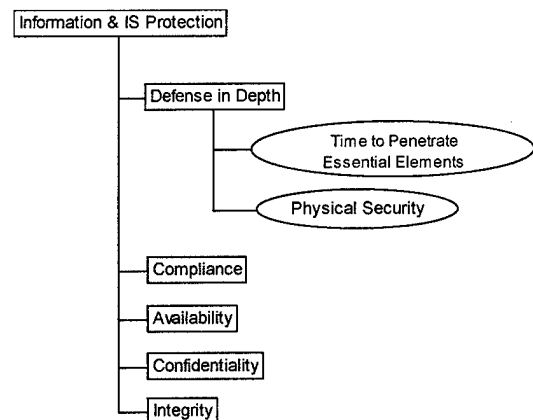
Defense in Depth are *Time to Penetrate Essential Elements* and *Physical Security*, which

evaluate the cyber and physical hardness of the information system respectively.

Time to Penetrate Essential Elements

This measure serves as a proxy for the virtual

hardness of the system. Essential elements are

defined as either information or information services

(functions) whereby a loss of availability, a breach of

confidentiality, or a breach of integrity would entirely

prevent or seriously degrade the organization's ability to perform its mission. Obviously, these

elements are organization and system specific. To implement this measure, an essential element

must first be identified. Second, risk assessment information should be utilized to determine

what type of attack, and the time required to carry it out, may be brought against the element.

Third, the time required protecting the essential element and returning it to its intended state

must be ascertained. This time, denoted as a *defense cycle*, is measured from initial detection,

and must include any process, mechanical and other reaction times necessary. Dividing the time

required for a successful attack by the time for a single defense cycle scores the defense in depth.

As a notional example, suppose that an intruder was detected, but five seconds thereafter

was able to peruse and modify classified databases because no other security controls were in

place (or effective) beyond that point. In order to stop the attack, the system administrator had to

log in (10 seconds), initiate the process to deny the intruder further access (30 seconds), and then

re-boot the system in order to restore the system to its original state to protect the system from a

ongoing attack (120 seconds)—a defense cycle of 160 seconds. Clearly, the time to execute a
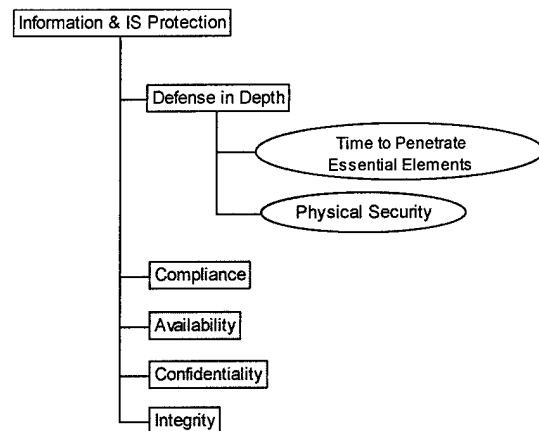
successful attack (5 seconds) is much faster than the time required to remedy the situation (160 seconds); a score of 5/160 (or 0.03) and an undesirable situation.
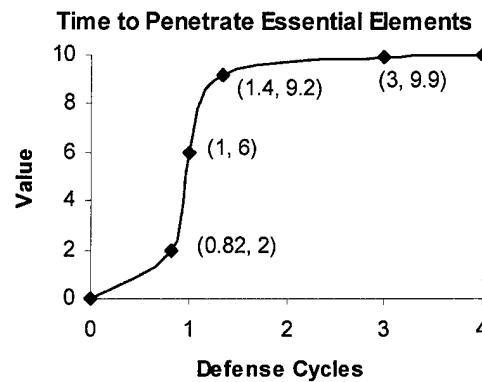
Figure A- 6: Value Function (VF) for Time to Penetrate Essential Elements

Enumeration of this function may be required to allow evaluation of multiple essential elements with either multiple levels of threat capability (or one worst case) against them. For example, if there were two essential elements of interest, and the organization wanted to evaluate the capability to protect against an amateur and a professional hacker, four evaluation measures would be developed. The weighting allocated to these four measures would then serve as a proxy for the probability of each of these scenarios occurring.

Physical Security

Physical Security measures the effective level of security afforded to network components of an IS. Physical security prevents unauthorized access to and tampering with IS components, which could result in a loss of availability, a breach of confidentiality, or a breach of integrity of information and IS functions to authorized users. The scope of physical control goes beyond IS
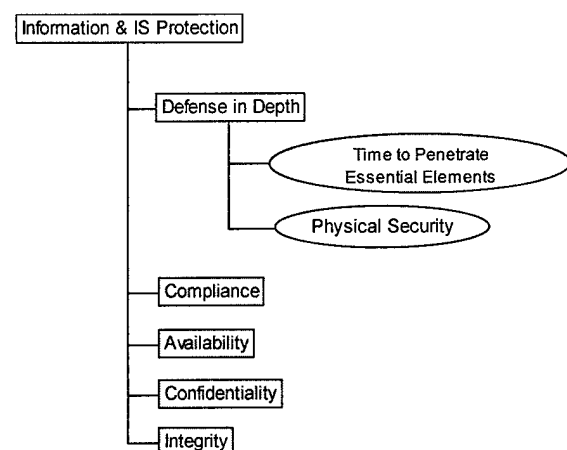
component accessibility. The processes that have a potential to expose information must also be protected (e.g. copiers, faxes, and computer screens). Similar to Doyle's offensive methodology, this measure evaluates the ease of defeating the physical hardness—"the ability of [a] weapon to penetrate or couple with [the information system]"—of the IS of interest. [1998:D-26] Assessments are limited to the physical assets that are within the span of control of the organization. This still leaves other physical points of access beyond the organization's control (e.g. transmission lines) vulnerable to physical attack. However, prior arrangements and cooperation with organizations that controls these supporting (or connecting) infrastructures may defend against them against physical attacks.

Typical actions taken vary from system to system and range from "nothing" to various physical-access controls (locks, combination doors, and perimeter security systems) and enforced manning policies (e.g. two-person integrity). [Doyle, 1998:D-26] Although these actions have varying strengths, their weaknesses lie primarily in the amount of time and rigor that is spent enforcing them. For example, if IS components are protected by a locked door and observed by authorized personnel during the day, but housekeeping has unlimited access during non-business hours, there exists a potential for unauthorized tampering that would result in a loss of availability.

With this in mind, there are several factors that must be considered in this "weakest link" approach: the perceived strength of the physical controls in place (or recommended), the amount of time in which they are enforced, and the level in which they are enforced through personnel awareness and automation. For the first consideration, it is assumed that the strength of the physical controls has been selected appropriately, commensurate with the value of information they are protecting. For the third consideration, it is assumed that personnel awareness

contributes to the timely detection of attempts to bypass physical security controls and is therefore evaluated in the *Detection* portion of the model. The second consideration—the amount of time in which the physical controls are enforced—is the one that can be measured and is directly related to the protection offered to information and information systems.

For each layer of physical protection, the probability of failure (P_{fail}) to prevent unauthorized physical access is dependent upon the type of physical control. If the physical control is not an electronic means that provides protection on a 24-hour, 7-day a week basis, then the time that authorized personnel enforce the controls is measured. This is based on the percentage of the number of hours in a week (i.e. 7x24=168) when personnel are present. For the lock and key example, if personnel authorized access to the IS work normal business hours during workdays, the P_{fail} equals $1 - (5x8)/168 = 1 - 0.238 = 76.2\%$. This method evaluates the potential opportunity an adversary may have to adversely affect the availability of information and IS to authorized users through physical manipulation of the IS itself. If the physical control is automated, providing continuous protection, then the P_{fail} is denoted by the demonstrated system reliability. Sample calculations are shown in Table A- 3.

To account for layered defenses, the overall P_{fail} is determined by estimating the probability of failure for each layer, and multiplying the probabilities together. For example, in order for a physical attack against availability to be successful, all security measures must be defeated. The probability of this occurring is the product of each layer's P_{fail}. In reality, the probability of failure of inner-layers must assume that an outer-layer has been defeated—suggesting that conditional probabilities would be more correct. However, the assumption of independence offers a conservative estimate of the overall P_{fail}.

Table A- 3: Sample P$_{fail}$ Calculations

Scenario	P$_{fail}$
BH-WD: Business Hours-Week Days (8x5/168)=23.8%	1 - .238 = 0.762
BH-AW: Business Hours-All Week (8x7/168)=33.3%	1 - .333 = 0.666
HD-AW: Half-Day (Extended Hours)-All Week (12x7/168)=50%	1 - .5 = 0.5
AD-AW: All Day-All Week (24x7/168)=100%	1 – System Reliability
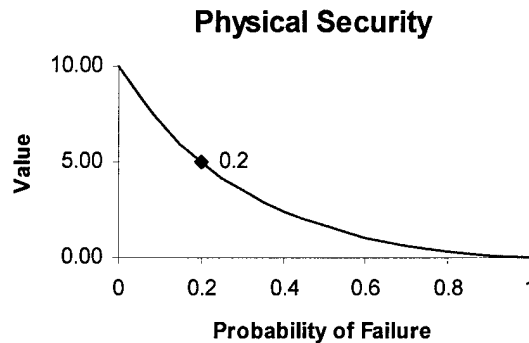
Figure A- 7: VF for Physical Security

Information & IS Protection: Compliance

Longstaff, et. al. noted that

"… in the late 1980s and early 1990s, the typical intrusion was fairly straightforward. Intruders most often exploited relatively simple weaknesses, such as poor passwords and misconfigured systems, which allowed greater access to the system than was intended. Once on a system, the intruders exploited one or another well-known, but usually unfixed, vulnerability to gain privileged access, enabling them to use the system as they wished." [Longstaff, et. al., 1997]
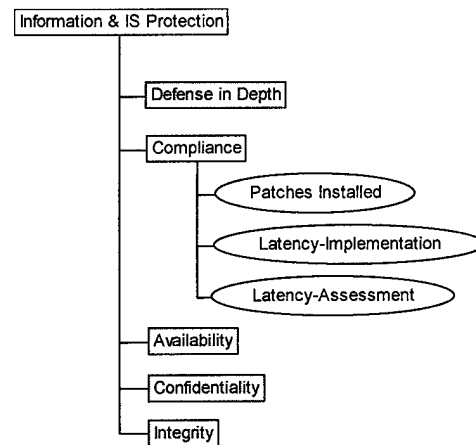
In an effort to impede the increasing trend of vulnerability exploitation, various computer emergency response teams (CERTs) have been instituted. The intent of these organizations is to disseminate information regarding vulnerabilities (and their potential impact) as well as the means to negate them if possible. If this information is applicable to the system of interest and

not implemented, then the system remains vulnerable. Unfortunately, a higher level of risk may be accepted, intentionally or unintentionally, in lieu of spending the time, effort and money involved to eliminate or reduce an identified vulnerability. Therefore, *Compliance* assesses the capability of the processes in place (or recommended) to accelerate the remediation of known vulnerabilities. These processes, automated or manual, are dependent upon an array of internal and external factors. Internal factors may include the level of staffing available to implement related efforts, while external factors might include how often (if at all) organizations with similar systems provide information on exploited vulnerabilities. Overall, the level of *Compliance* process provides value to the decision-maker by directly protecting information and IS and by capitalizing upon the lessons learned by other.

The overall objective is to maximize compliance, which helps to maximize vulnerability reduction through complying in three measures: *Patches Installed*; *Latency-Implementation*; and, *Latency-Assessment*.

Patches Installed

This evaluation measure determines the extent to which any applicable known system vulnerabilities have been reduced or eliminated. Patches, in this case, primarily includes software installations, software modifications, and software settings recommended by vendors, CERTs and other agencies in order to prevent the exploitation of known vulnerabilities. Note that these patches may protect the availability, confidentiality, integrity or all of these aspects of the information and IS. To implement this measure, the system is scored by assessing the percentage of patches

A-15
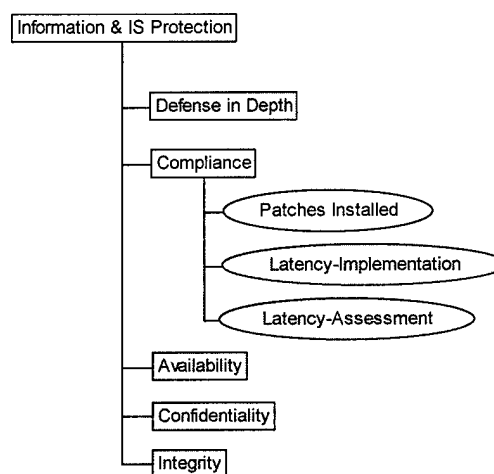
implemented that are applicable to the system of interest. Table A- 4 shows the magnitude to which these types of vulnerabilities are growing. Obviously, not all of these vulnerabilities may be applicable to the system of interest, but the lack of an efficient process to eliminate or reduce the ones that are may be a costly mistake.

Table A- 4: Vulnerabilities Reported [CERT, 2000]

Year	1995	1996	1997	1998	1999	**Total**
Vulnerabilities	171	345	311	262	419	**1508**
Source: CERT/CC Statistics [www.cert.org/stats/cert_stats.html]						

It is initially assumed that the implementation of each patch contributes an equivalent amount of value, suggesting a straight line for the evaluation function. Future studies, however, given a system's list of known vulnerabilities are prioritized by the level of risk, may change this evaluation measure to the percent of risk mitigated by patches installed.

Patches Installed

Value

% Applicable Patches Implemented
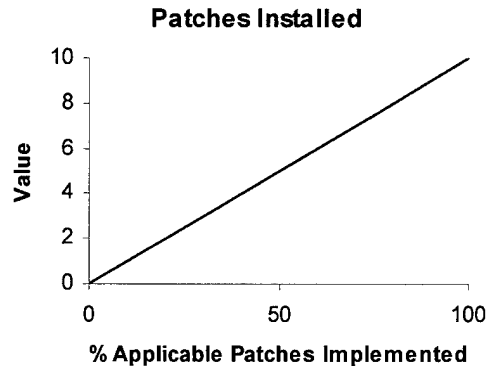
Figure A- 8: VF for Patches Installed

Latency-Implementation

This evaluation measure denotes the age of the oldest known vulnerability (applicable to the system) that has not yet been implemented. This assumes that a countermeasure exists and is available to the organization. This measure evaluates how well the system is being maintained in the sense that the longer an IS remains open to attack, the longer an unneeded risk prevails. Processes supporting the expeditious implementation of countermeasures of known vulnerabilities are preferred. From Figure A- 9, the timeliness (or lack thereof) of these processes will either reduce or extend the time the information and information systems are vulnerable, thus shrinking or expanding the 'length' of the figure.
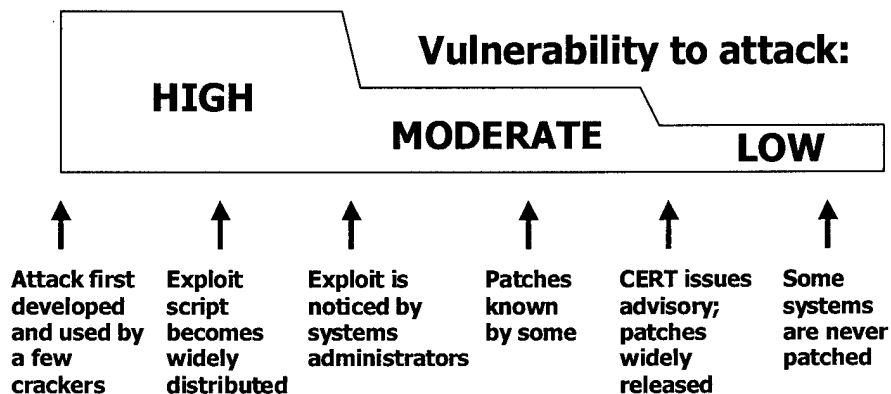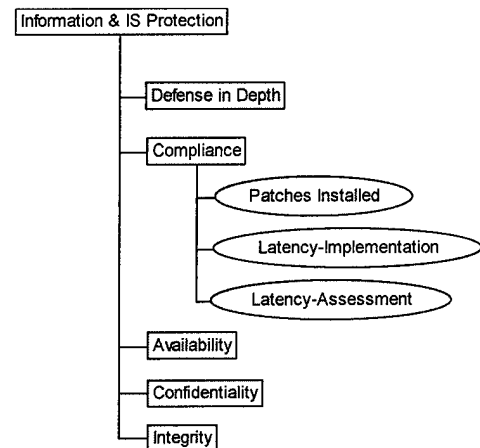
Figure A- 9: Vulnerability over Time [Kendall, 1999:27]

Implementation of this measure is accomplished by reviewing the list of all identified vulnerabilities that have not yet been implemented. Of these vulnerabilities, the time elapsed since each was first discovered is assessed. A shorter duration implies that the processes are in place and are being effectively executed in order to reduce known vulnerabilities. Longer

A-17

duration implies that either internal or external processes are inefficient in implementation or reporting respectively, and must be addressed. It is assumed that a system with vulnerabilities older than 6 months have processes of little value to decision-makers that must be reviewed and improved.

Latency in Implementation
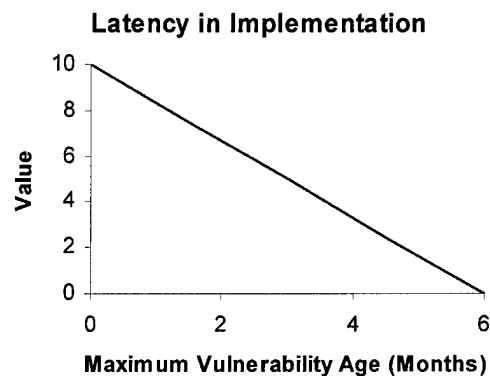
Figure A- 10: VF for Latency-Implementation

Latency-Assessment

The final measure proposed to evaluate the level of *Compliance* is *Latency-Assessment*. This addresses the overall state of vulnerability of an organization and its information and IS. For Air Force systems, current regulations mandate a formal evaluation be accomplished every three years. [AFSSI 5024, Vol.1, 1997:7] However, the rapid growth of technology offering new and improved capabilities also brings new vulnerabilities. Therefore, any process to more frequently update the 'list' of patches applicable to the system, "continuously identifying and analyzing threats and vulnerabilities to the information system and its information to maintain an appropriate level of protection" provides
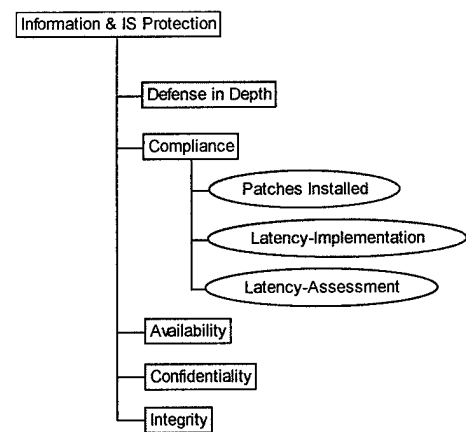
value to the decision-maker. [AFI 33-202, 1999:6] There are varieties of means to accomplish

this task. A report from the Information Assurance Technology Analysis Center (IATAC)

discusses a variety of tools used to facilitate these processes; a summary is shown in Table A- 5.

Table A- 5: Vulnerability Analysis Tools

Description and Types of Vulnerability Tools
Simple Vulnerability Identification and Analysis
These tools provide limited capability, performing configuration checks and automating scanning and response functions.
Comprehensive Vulnerability Identification and Analysis
These tools provide more sophisticated and comprehensive "in terms of the scope of vulnerabilities addressed, the degree of analysis performed, and the extent of recommendations made to mitigate potential security risks." [IATAC, 1998a:4]
War Dialers
This tool dials a range of telephone numbers in search of a modem that provides a login prompt in order to find potential "back doors" to the system.
Password Crackers
These tools support enforcement of password selection policies.
Risk Analysis Tools
These tools "provide a framework for conducting a risk analysis, but do not actually automate the vulnerability identification process." [IATAC, 1998a:4]
Source: IATAC. *IA Tools Report: Vulnerability Analysis.* Spring 1998

The resulting value function is shown in Figure A- 11.
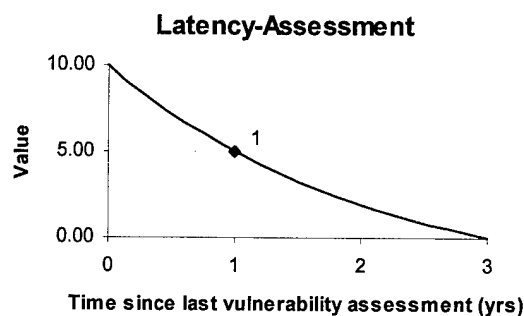
Figure A- 11: VF for Latency-Assessment

It is assumed that waiting to identify new vulnerabilities until the 3-year point provides

little or no value to the decision maker, particularly the designated accreditation authority

A-19

(DAA), who assumes the risk associated with the operation of an information system. Frequent assessments of system vulnerability, internal or external, and regardless of the means, will provide more value to the DAA by affording the opportunity to reduce or eliminate new vulnerabilities.

Information & IS Protection: Availability

The requirement for availability applies to both the information and information systems. For example, a threat may destroy information while leaving the information system intact, deny the use of the information system to authorized users, or destroy information that renders the information system useless. Actions to ensure access to information and information systems must protect against these types of attacks. Means to ensure availability include building extra capacity and/or capability, maintaining the system configuration to preclude successful exploitations of known vulnerabilities, as well as physically securing network components to avoid unauthorized tampering or destruction.
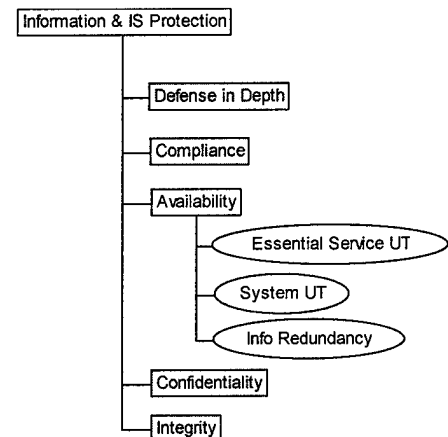
Protection of information and information system availability is of considerable concern. Denial of service (DoS) attacks are becoming increasingly prevalent, and can be devastatingly costly, particularly to entities such as Internet Service Providers (ISP) or military organizations during time of conflict or heightened operational tempo. These costs may include financial losses, lack of confidence, distrust, and most critically, loss of life. The CERT has observed a variety of forms of attack against an array of services. These attacks fall into three basic types: Consumption of scarce, limited, or non-renewable resources; destruction or alteration of configuration information; and, physical destruction or alteration of network components.

A-20

[CERT/CC, 1999] CERT also notes "physical security is a prime component in guarding against many types of attacks in addition to denial of service." [CERT/CC, 1999]

This section discusses the first area, identifying the value of *Availability* through *System Resiliency* and its contribution to protecting the availability from not only intentional threats, but natural threats as well. The other areas dealing with physical security and system configuration are already measured under *Defense-in-Depth* and *Compliance* discussed earlier.

The goal of protecting availability is to ensure that authorized users have operationally effective access to information when required. As stated earlier, this objective assesses the reliability built into (or added onto) the system. Reliability, formally defined as "the probability that it will survive fully functional throughout a particular time span," denotes the overall reliability of the information system. [Lapin, 1990:690] System reliability provides a direct measure of the availability of the IS to authorized users. IA strategy implementation may improve or degrade the overall IS reliability due to the addition or deletion of components or the introduction of cutting-edge, yet immature, technologies. This assessment of the system resiliency will serve as a proxy for the protection of Availability, which characterizes the potential for ongoing use of the system, regardless of threat activities, through protection against the "consumption of scarce resources" while indirectly protecting against "the physical destruction or alteration" of network components. The evaluation measures are *Essential Service Uptime* (UT), *System UT*, and *Information Redundancy*.

Essential Service UT

This measure assesses the percent of time that essential services are available to authorized users, under normal conditions. Essential services are specific to each organization and their mission. Normal conditions imply that the system is being used in the manner for which it was designed.
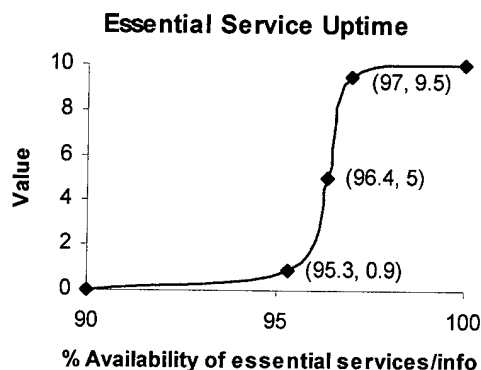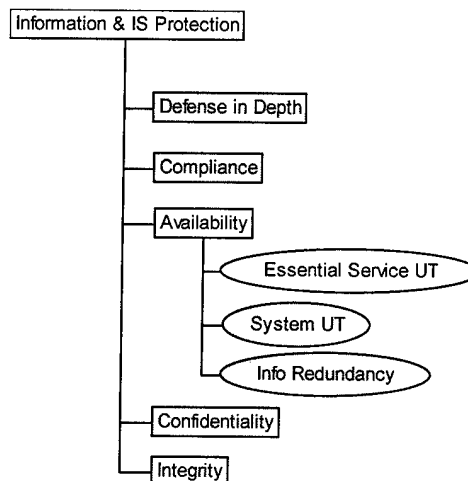
Figure A- 12: VF for Essential Service Uptime

System UT

This measure assesses the percent of time that the system and all its services are available to authorized users under normal conditions. Normal conditions imply that the system is being used in the manner for which it was designed.

Overall System Uptime
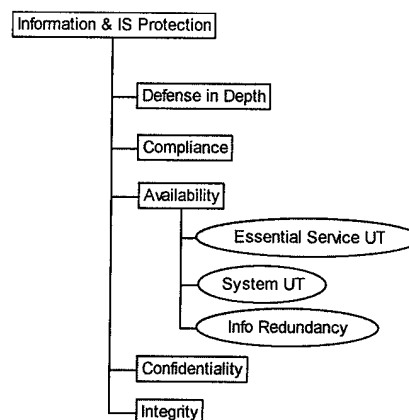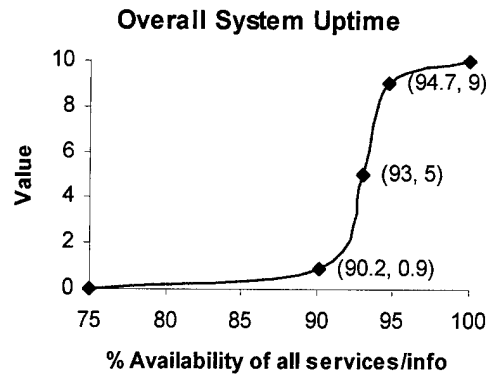
Figure A- 13: VF for System Uptime

Information Redundancy

Redundancy may be seen in the information itself
and throughout the IS. Redundancy complements
reliability, however it is a distinctly separate concept in
that either it exists or it does not. With respect to
information availability, *information redundancy*
strengthens 'fault tolerance,' which "protects [the availability of information] by storing [it] on

several devices in different locations. This helps ensure users will be able to access important

information even if one storage device fails." [Whitehead, 1997:176] Methods of dispersing and

storing information vary, as does the subsequent level of protection. *Information redundancy*

also ensures that alternative locations of information are available to authorized users, in the

event that either information is destroyed or access is eliminated or severely degraded by a

threat. The number of locations of information sources will serve as the measure for *information*

redundancy. This measure assumes that each source is independent from and identical to all

others, within operationally acceptable limits. Such limits are dependent upon system-specific

characteristics and the criticality of the information involved. The potential range of the number

A-23
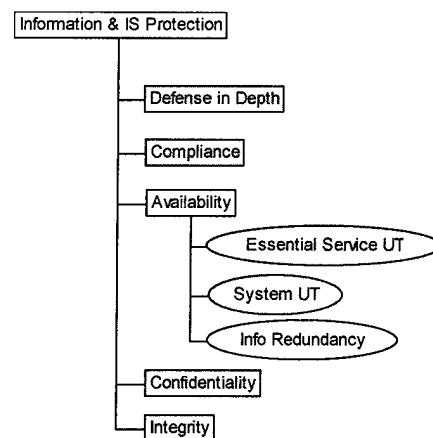
of data sources, currently one to four, may change from system to system, depending upon its intended use. For example, highly classified information may limit the number of backups due to the increased opportunity for unauthorized disclosure. It is assumed that more than four sources are neither cost nor operationally effective.

Information Redundancy
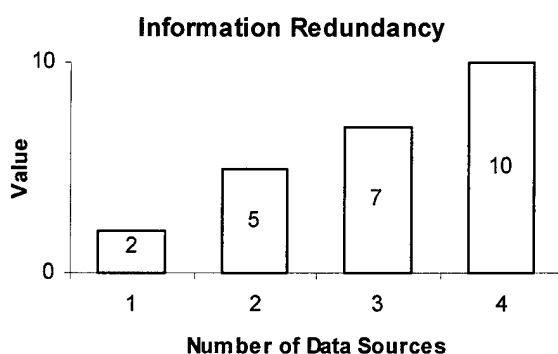
Figure A- 14: VF for Information Redundancy

Information & IS Protection: Confidentiality

Confidentiality is defined as "assurance that information is not disclosed to unauthorized persons, processes, or devices." [NSTISSI 4009, 1999:12] Maintaining confidentiality of information and information systems provides value to decision makers by preventing certain types of information from being used against their own forces or by preventing the disclosure of high-value information sources.
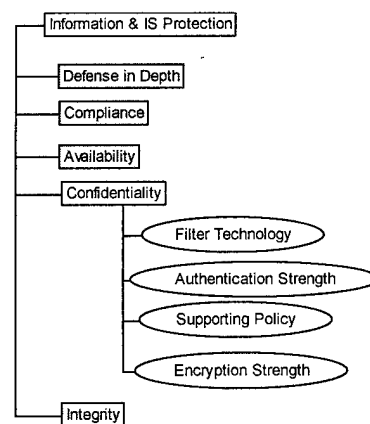
In the context of this document, unauthorized disclosure, regardless of whom it is disclosed to, can occur in one of two ways: through vulnerabilities or weaknesses in the electronic connectivity or operation of information systems, or through vulnerabilities or weaknesses in the physical access to the information system itself. Categorizing these areas as

A-24

virtual and *physical* respectively, the objectives will be to maintain control of any associated vulnerability within either of these two areas. Security disciplines like Emissions Security (EMSEC), Communications Security (COMSEC), Computer Security (COMPUSEC) and physical security are examples of current practices that contribute to the level of control maintained over these domains. [AFI 33-202, 1999:3] This area focuses on preventing a breach of confidentiality via exploitations of virtual means. Maintaining confidentiality of information and information systems through physical means is accounted for in the *Physical Security* measure of *Defense in Depth* discussed earlier. It is also important to note that while some means of protecting confidentiality may contribute to the *Defense in Depth* of a system, it is the overall combination of technologies and procedures that provide protection through depth. The following evaluation measures focus specifically on protecting the confidentiality of the IS and the information within.

Protective actions must account for system-specific vulnerabilities as well as inter-system vulnerabilities. System-specific protection measures prevent unauthorized disclosure in two ways: (1) by preventing individuals that have no level of authorization (outsiders) access to the system and its information, and (2) by preventing individuals that have some level of authorization (insiders) access to information that is beyond their intended privileges. Examples include a number of access-control devices, various means of identification and authentication (*I&A*), and vulnerability assessments to identify (and remedy) potentially damaging weaknesses in system configuration. Inter-system protection prevents unauthorized disclosure by protecting information in-transit, either by cable or wireless methods. Examples include encryption and virtual private networking. The *I&A* process also supports inter-system protection by establishing 'trusted' relationships between the authorized users on different systems.

This leads to four evaluation measures that assess the level that confidentiality is protected: *Filter Technology, Authentication Strength, Supporting Policy* and *Encryption Strength*.

Filter Technology

To protect the confidentiality of a system and its information, the typical first line of protection is some method of access control. These controls comprise "a component or set of components that restricts access between an protected network and an unprotected network, or between other sets of networks and facilitates authorized access to protect network resources through proxies, filters, and other mechanisms," [IATAC, 1998:1]. As far as protecting confidentiality, the effectiveness of these systems is dependent upon the mechanism type and its configuration, as well as the origin of the threat. The primary purpose of these controls is to prevent outsiders from obtaining access to information and IS services. Unless these mechanisms are implemented to specifically differentiate among users that have some level of authorization, they cannot protect a system from an 'insider threat.'

The IATAC categorizes the filtering technologies used to build firewalls into three types, in order of security provided: packet filtering, circuit-level gateways, and application-level gateways. These techniques differ primarily in the level of "access control granularity" provided, their cost and their capabilities. Currently, combinations of these techniques are being used to improve protection capabilities—referred to as 'hybrid' systems. [IATAC, 1998:2] As with any other network component, updates and identified vulnerabilities must be maintained,
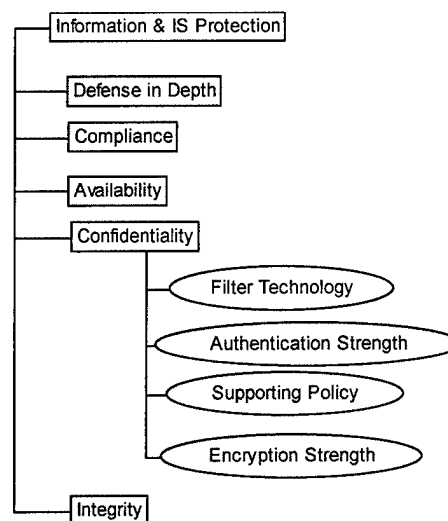
which are accounted for in the *Compliance* objective discussed earlier. Considering the

multitude of factors involved, the type of filter technology is used as a proxy for the protection

afforded to the confidentiality of the IS and its information.

Filtering Technology
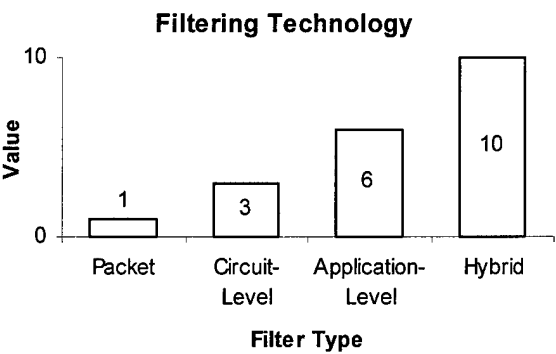
Figure A- 15: VF for Filter Technology

Other factors to consider include layering of defenses, as well as the location of

information requiring confidentiality with respect to these defenses. As discussed earlier, these

issues should be accounted for in the *Defense in Depth* assessment. Note that a conservative

'weakest link approach' may also be used if there are multiple access points into the IS/network.

If a layered approach is taken, a probabilistic assessment of all layers failing to maintain

confidentiality may be used, as shown in the evaluation of *Physical Security* discussed earlier.

Authentication Strength

Identification is "the process where individuals identify

themselves to a system as a valid user." Authentication is "the

procedure where the system verifies the user has a right to access

the system." [AFMAN 33-223, 1998:2]

Currently, *I&A* methods can be grouped into the four

general categories described in Table A- 6. The methods are listed
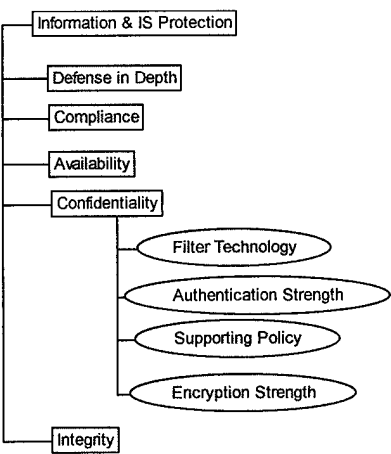
in the order of their perceived strength, or the difficulty associated with fraudulently imitating an authorized user's identity.

Table A- 6: *I&A* Methods

Identification and Authentication Methods [AFMAN 33-223, 10]	
Knowledge-Based	Requires the user to provide a pre-established piece of information in order to gain access. The authentication succeeds if the information provided by the user matches what the system expects. This method assumes that the user is the only one who knows what is expected, thereby identifying the individual.
Possession-Based	Requires the user to produce a physical token that the system can recognize as belonging to a legitimate user. These tokens typically contain physical, magnetic, or electrically coded information recognizable to the host system, thereby requiring a threat to counterfeit or steal a valid token to gain access.
Biometrics-Based	Rely upon a unique physical characteristic to verify the identity of a user. Common identifiers include fingerprints, voice patterns, retinal scans, and hand geometry. This method often requires expensive hardware, but offers a very high level of security.
Combination	Combinations of I&A techniques make it much more difficult for the perpetrator to obtain the necessary items for access. Automated teller machines have the most widespread use of this technique, combining the possession- and knowledge-based methods.

Cost-efficiency and ease of implementation have led to the "user-ID" and password as the most common *I&A* knowledge-based technique. Unfortunately, their "vulnerability to interception or inadvertent disclosure" also make them the weakest method—inappropriate passwords comprise the most common IS vulnerability. [AFMAN 33-223, 1998:2] Air Force official guidance also notes that "passwords are only effective when used properly," suggesting that complementary policies and practices are required. [AFMAN 33-223, 1998:2]

The type of *I&A* method used will serve as a proxy for the strength of the system's capability to accurately identify and authenticate users and their appropriate levels of access.
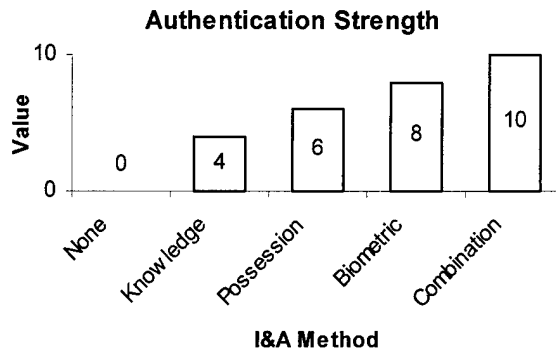
Figure A- 16: VF for Authentication Strength

Supporting Policy

An additional measure that supports the strength of authentication is that of supporting policy. This assesses supporting policy that may complement the *I&A* methods to ensure that the methods are being implemented correctly. An example would be an automated policy enforcing 'appropriate' passwords (i.e. includes numbers, special characters, etc.). Points that must be considered include restrictions on password content and use, configuration of machines to comply with *I&A*, interoperability, and other methods that enhance/ensure proper user use of the *I&A* methods implemented. The four levels for this measure includes *No Policy, Policy-No Checks, Policy-Periodic Checks*, and *Policy-Automated Checks*. *No Policy* means that no policy supporting the *I&A* processes exists. *Policy-No Checks* means that supporting *I&A* policy exists, but there are no checks on whether it is ignored or not. *Policy-Periodic Checks* means that a supporting *I&A* policy exists, and manual checks for adherence to the policy are accomplished on a periodic or
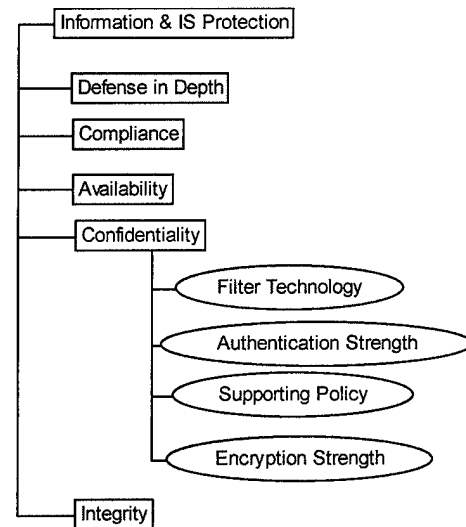
as-needed basis. *Policy-Automated* means that a supporting *I&A* policy is in place and enforced by automatic means.
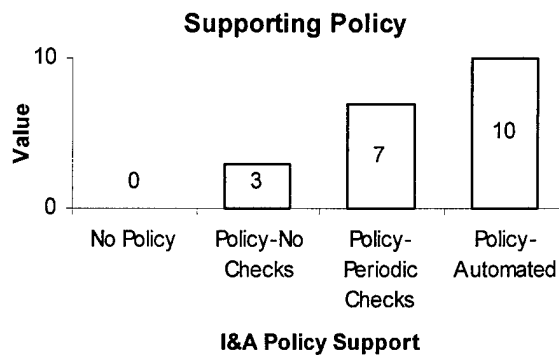
Supporting Policy

Figure A- 17: VF for Supporting Policy

Encryption Strength

When information is in transit, the sender may have little or no control over where it flows en route to its destination as well as the media in which it flows. Therefore, encryption technology has provided a means to protect the confidentiality of information if unauthorized parties intercept it. However, this

technology is not without its own vulnerabilities. The Public Key Infrastructure (PKI) technology is, like all other network-related technologies, rapidly growing in capability. Therefore, instead of directly using the encryption strength as a measure of assurance against a breach of confidentiality of information in transit, the generation of technology will be assessed. This approach assumes that the necessary precautions are taken in order to prevent the encryption keys from being revealed. This measure has five levels: *None, Two Generations Past, Last Generation, Current Generation, and State of the Art Generation. None* means that

A-30
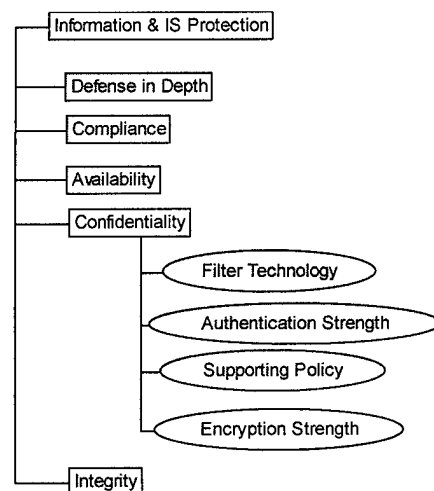
no encryption is used for sending information to others. *Two Generations Past* (2 Past) denotes

the use of encryption that has been succeeded by two generations of encryption technology (e.g.

32-bit). *Last Generation* denotes the version of encryption that was widely used before the

current generation (e.g. 64-bit). *Current generation* denotes the use of the most current version

of encryption that is widely disseminated (e.g. 128-bit). Widely disseminated is further defined

as encryption technology used by at least 75% of the Internet population that uses encryption.

State of the Art generation denotes the most advanced version of encryption available but not

widely used for developmental, proprietary, regulatory or validation reasons (e.g. 640-bit or

higher). It should be noted that as more advanced encryption become available the definitions,

although not the illustrative example, will remain valid.

Encryption Strength
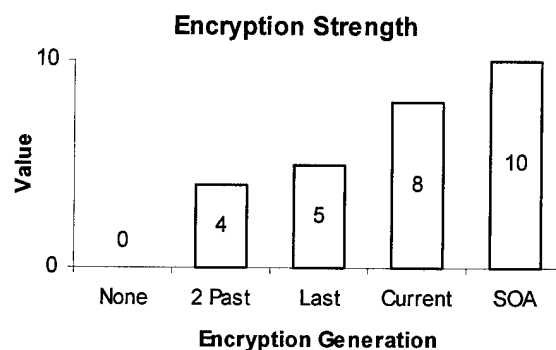
Figure A- 18: VF for Encryption Strength

Information & IS Protection: Integrity

Integrity addresses two distinct areas: data integrity

and system integrity. Data integrity is defined as the

"condition existing when data is unchanged from its source

and has not been accidentally or maliciously modified,

altered, or destroyed." [NSTISSI 4009, 1999:15] Whereas,

A-31
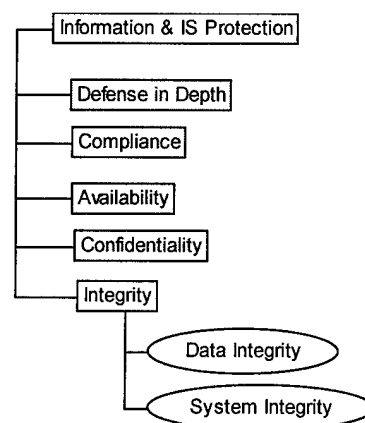
system integrity is defined as "the state maintained when an IS "performs its intended function in

an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the

system." [NSTISSI 4009, 1999:44] It is important to note that a loss of data integrity may

contribute to a loss of system integrity. However, to achieve mutual exclusivity between these

two areas, *Data Integrity* will apply only to the protection of information in a virtual sense, and

System Integrity will apply only to the protection of the IS in a physical sense.

<u>*Data Integrity*</u>

There are several methods to prevent the loss of data
integrity. Discretionary access control (DAC), for example,
"provides the ability to control a user's access to information
according to the authorization granted to the user," and is
administered by the individual users themselves. [AFMAN 33-
229, 1997:5] DAC and its strength are dependent upon the operating system's capabilities and

whether or not it is effectively implemented by IS users. It is important to note, "all Air Force

shared (i.e., multi-user) information systems must have DAC based on the requirements levied

by Public Law 100-235, NTISSP 200, DOD Directive 5200.28, and AFSSI 5102." [AFMAN

33-229, 1997:5] Therefore, for the purposes of this analysis, it is assumed that the system meets

the legal requirements with respect to this area.
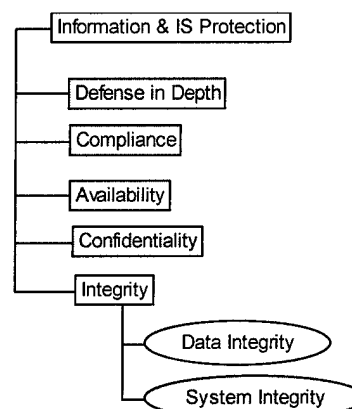
Another means is that of open source software. This approach allows users to know

exactly what a software package contains and the functions it performs. This method, however,

is not a widely accepted practice. In addition, if a software package consists of millions of lines

of code, identification of one or two lines of malicious code may be a daunting task in itself.

An additional means, the focus of this evaluation area, is the use of anti-virus software to maintain data integrity. The strengths of which rely upon how it is used (i.e. manually or in an automated fashion), how often the malicious code signatures are updated (to allow for detection, eradication and notification), and the type of coverage offered to the IS as a whole. Coverage considers the extent of protection offered against the potential sources of malicious code. Figure A- 19 illustrates these sources, which are denoted as external, internal and originating sources.

External sources of malicious code come from outside of the IS of interest, and infect the system by passing through inadequately maintained protective barriers. This may occur directly from source to target or from source to a target through a series of systems that are also inadequately protected. Internal sources stem from users placing malicious code (intentionally or unintentionally) on a computer within the IS and its boundaries to the outside world.
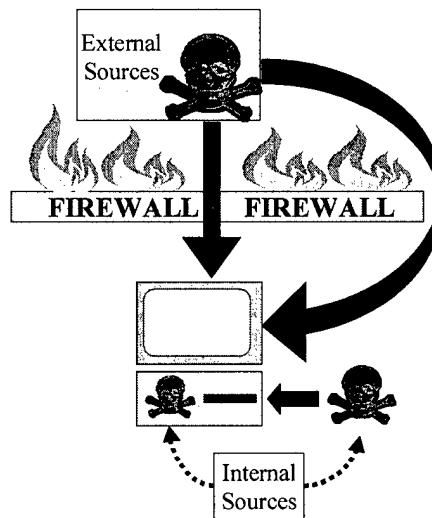
Figure A- 19: Potential Sources of Malicious Code

Assuming the capability exists to identify the malicious code, the speed, accuracy and ability to mitigate the code's damage are all aspects that require consideration. Due to the multitude of factors involved, and the system-specific complexities of this area, a categorical

measure was developed, essentially measuring the protection afforded to data integrity by assessing the strength of the *Implementation* against malicious code.

The five levels for this measure include: *None, Manual-Partial, Automated-Partial, Manual-Full,* and *Automated-Full. None* means that no anti-virus (AV) or integrity-checking software is implemented within the IS. *Manual* means that the AV or similar software is in place but relies upon human intervention to implement its use, to include any updates required. *Automated* means that AV or similar software is in place and does not rely upon human intervention to implement its use, to include any required updates. *Partial* means that not all points of access are monitored for malicious code; whereas, *Full* means that all points of access are monitored for malicious code. The combinations for the measure are ordered by preference, assuming that *Full* coverage is preferred to *Partial* coverage, regardless of how the protective measures are implemented.
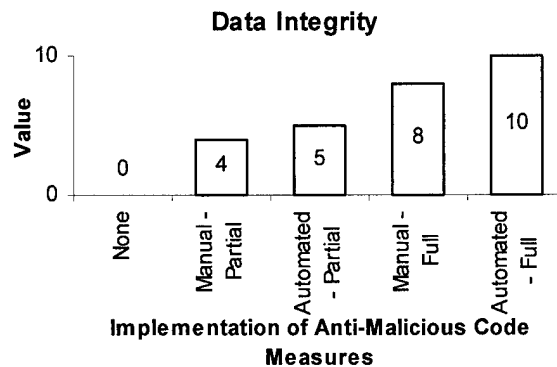
Figure A- 20: VF for Data Integrity

Finally, originating sources include the intentional or inadvertent breach of integrity through improperly evaluated hardware or software components that are added onto the IS. The specificity to IS components resulted in evaluation in the context of maintaining system integrity.

A-34

IS Integrity

In this analysis, protecting system integrity "from deliberate or inadvertent unauthorized manipulation" is limited to the protection of the physical components that comprise (or may comprise) the information system of interest. Protection of the integrity of infrastructures that directly support the IS (e.g. electrical, or communication lines) is considered beyond the scope of this thesis. However, the proposed model could allow for these considerations within the *Defense in Depth* assessment.[2] Therefore, this portion of the model assesses the protective actions taken to prevent not the alteration of components, but to prevent the introduction of altered components into the information system.
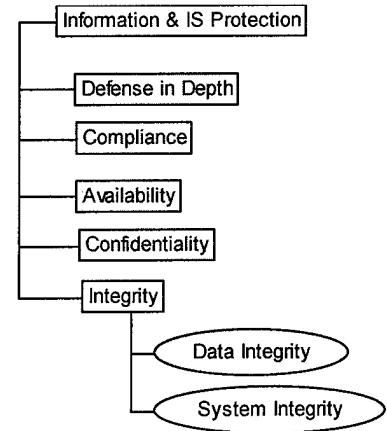
DOD Instruction 5200.40 mandates the validation of all system components (hardware, firmware and software) to assure proper integration and that system-specific functionality and security needs are met. [DODI 5200.40, 1997:28] The level of resolution attained by breaking systems down into individual components is dependent upon the organization and the function of the IS. For Air Force systems, AFISSI 5024, Volume 1 further requires security controls (software or hardware) are "tested and evaluated to ensure they are implemented as required by DOD and AF policy." [1997:56] Products validated by the National Security Agency (NSA) are lists as such on an evaluated products list (EPL), which also denotes the class (or classes) of system for which the product is approved. Products assessed by the Air Force, are listed on the assessed product list (APL), which describes the results of testing but does not directly state on

which systems the product may be used. In the event that system specifications require a new product not yet tested, a test may be requested or accomplished by the organization. Unfortunately, this process is time intensive, taking up to a year to complete. [1997:57]

From this, an IA strategy with pre-approved components is assumed preferable, at least in the short term. Therefore, the percentage of components already validated serves as a proxy for system integrity. Long-term acquisitions may allow long testing times in order to achieve an improved capability. Unfortunately, time works against the decision-maker due to the rapid evolution of information technologies, hence a dramatically reduced value for any alternative with less than 85% of the components already validated. Although it is expected to be 100% for the current system, the evaluation process for this measure should lend itself to verifying this as the case.
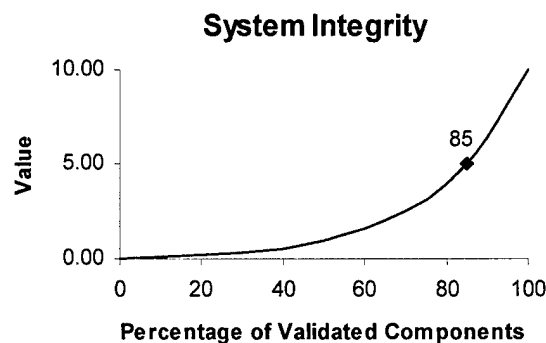
System Integrity

Figure A- 21: VF for System Integrity

---

[2] Protection of supporting infrastructure is what relates information assurance directly to critical infrastructure protection.

Detection

"History has shown the value and
need for reliable, adequate, and timely
intelligence, and the harm that results from
its inaccuracies and absence." [JP 3-13, 1998:III-5]

```
          ┌──────────────────────┐
          │ Information Assurance │
          └──────────────────────┘
    ┌───────────┴──────────┬───────────────┐
┌──────────────────────┐ ┌───────────┐ ┌──────────┐
│ Information & IS Protection │ │ Detection │ │ Reaction │
└──────────────────────┘ └───────────┘ └──────────┘
```

In light of the historical perspective of 'detecting' enemy actions, Joint doctrine also

emphasizes, "timely attack detection and reporting are the keys to initiating capability restoration

and attack response." [JP 3-13, 1998:III-10] In addition to timely detection, effective defense

against IO "… is predicated on how well the intelligence processes function and on the agility of

[those involved] to implement protective countermeasures." [JP 3-13, 1998:III-2] This suggests

that a certain level of reliability is required to ensure that threats are indeed identified—

maximizing the probability of detection and minimizing the probability of false alarms.

Additionally, an effective IA strategy must also be robust in that it exhibits timeliness and

reliability, regardless of the type of attack. The resulting value hierarchy for *Detection* is shown

below.

```
┌───────────┐
│ Detection │
└───────────┘
    │  ┌────────┐
    ├──│ Timely │
    │  └────────┘
    │     │  ┌──────────────┐
    │     ├──│ Cyber Attacks │
    │     │  └──────────────┘
    │     │  ┌─────────────────┐
    │     ├──│ Physical Attacks │
    │     │  └─────────────────┘
    │     │  ┌──────────────────────┐
    │     └──│ Inter-Personal Attacks │
    │        └──────────────────────┘
    │  ┌──────────┐
    └──│ Reliable │
       └──────────┘
          │  ┌──────────────┐
          ├──│ Cyber Attacks │
          │  └──────────────┘
          │  ┌─────────────────┐
          ├──│ Physical Attacks │
          │  └─────────────────┘
          │  ┌──────────────────────┐
          └──│ Inter-Personal Attacks │
             └──────────────────────┘
```
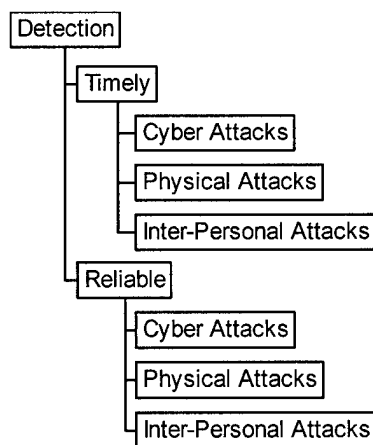
Figure A- 22 – Values of Detection Capability

There are many means of accomplishing an attack upon information and information

systems. As discussed earlier, *virtual (or cyber) attacks* exploit connectivity or operation (i.e.

emissions or information in transit) to gain unauthorized access (by either an authorized or unauthorized user) and attack information and/or information systems. *Physical attacks* exploit accessibility to information system components and attacks information and/or information systems by unauthorized modification, destruction, or subversion. A third category of attack not yet discussed—*inter-personal attacks*—involves the exploitation of training and/or awareness deficiencies of the individuals that operate, maintain or use the IS and the information that resides within it. For the purposes of this research, assessing an IA strategy's detection capability is accomplished through quantifying its capability to detect attacks in a timely and reliable manner in each of these three areas.

Timely (Cyber Attacks)

As stated earlier, regardless of the type of attack, the earlier an attack (or intrusion) is detected, the quicker an appropriate response can be initiated. However, due to the speed at which cyber attacks may be accomplished, timeliness is a vital factor.

Detection

- Timely
  - Cyber Attacks
    - Internal
    - External
  - Physical Attacks
  - Inter-Personal Attacks
- Reliable
  - Cyber Attacks
  - Physical Attacks
  - Inter-Personal Attacks

Detection speeds of current systems are heavily system dependent. Kendall summarizes "some systems detect attacks in real time and can be used to stop an attack in progress. Others provide after-the-fact information about attacks that can be used to repair damage, understand the attack mechanism, and reduce the possibility of future attacks of the same type." [1999:8]

Figure A- 23 depicts the four categories of intrusion detection approaches. The approach on bottom can only identify previously demonstrated attacks, whereas the three on top are capable of identifying new attacks. As the graph extends to the right, so does the computer power required to successfully implement the detection approach.
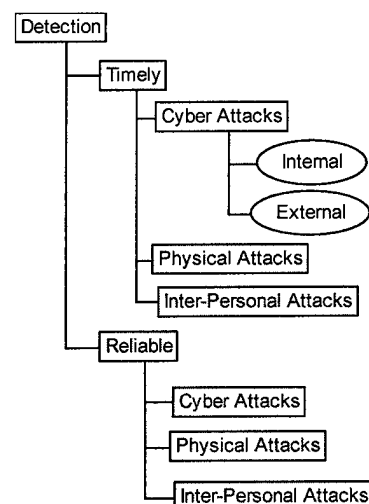
Signature verification relies upon identification of "an invariant sequence of events that match a known type of attack." This approach can be very effective against previously demonstrated attacks; however, "it is difficult to establish rules that identify novel types of attacks," and may be subject to high false alarm rates. [Kendall, 1999:16]
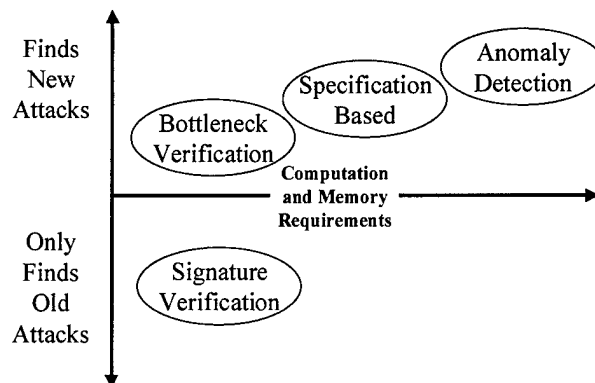
Figure A- 23: Strategies for Intrusion Detection [Kendall, 1999:16]

The three other approaches were developed to overcome these shortfalls. Bottleneck verification "applies to situations where there are only a few, well defined ways to transition between two groups of states." The transition from user to super-user[3], for example, can be identified and tracked for illegal actions, regardless of the means (new or old) that the transition is accomplished. [Kendall, 1999:19] Specification-based detection focuses on the improper use of system or application programs by comparing their activity to the normal intended behavior of the programs. [1999:18] Although this approach detects a wide range of attacks at a low false alarm rate, it requires application-specific, written security specifications that must be updated along with the associated program. The final category of current approaches is anomaly detection. This approach "constructs statistical models of the typical behavior of a system and

---

[3] Special users who can perform control of processes, devices, networks, and file systems. [NSTISSI 4009, 1999:43]

issues warnings when they observe actions that deviate significantly from those models."
[Kendall, 1999:17] In order to minimize the false alarm rate, careful training must be
accomplished to separate anomalous behavior from attack events. This may be difficult to carry
out for all types of users. Additionally, an adept adversary may be able to slowly change the
model (undetected) over time to allow a complete and undetected attack in the future. [1999:18]

In addition to the specific components of an information system dedicated to intrusion
detection, JP 3-13 identifies other elements of IO attack detection. These include Information
Warfare Centers, Information Systems Developers, Information Systems Providers and Systems
Administrators, Information and IS Users, Law Enforcement, Intelligence and the reporting
structure through which these entities share information regarding impending or ongoing attacks.
[1998:III-10-12] This means that the time required for detection is dependent upon the method
of detection and the organizational level of detection. The reporting of intrusion detection by the
upper echelons or cooperating agencies also relies upon their own detection capabilities, as well
as the efficiency of the reporting process. For this thesis, the scope of assessment is constrained
to the system of interest and its capability (current or proposed) to detect intrusions in a timely
manner. This evaluation measure has four levels: *No Capability, Post-Attack Only, Real-Time
(On Duty)*, and *Real-Time (Off-Duty)*.

No Capability means that there is no capability to detect cyber intrusions into the system.
Post-Attack Only means that the organization can only detect intrusions 'after the fact,' using
manual or automated means, accomplished during a timeframe specified by the security policy.
Real-Time (On Duty) means that the organization has the capability to detect intrusions on a real-
time basis, but appropriate personnel are only notified of the intrusion during duty hours. *Real-
Time (Off Duty)* means that the organization has the capability to detect intrusions on a real-time

basis, and appropriate personnel are automatically notified regardless of their duty status (e.g. 24-hour alert status).

This evaluation measure is applied to the assessment of the detection capabilities of both internal and external threats. However, an independent assessment of each threat type must be accomplished, due to the different means of detection, or the configuration of the system, must accommodate for the detecting the different types of adversaries.

Internal Detection (Timely)
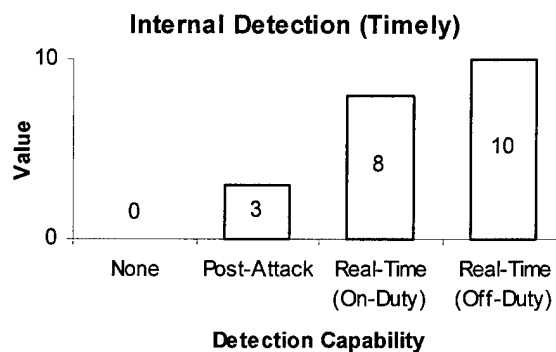
Figure A- 24: VF for Timely Detection of Internal Threats

Timely (Physical Attacks)

The timely detection of physical attacks is dependent upon the level of sophistication of the controls in place as well as the level of awareness of authorized personnel. More sophisticated controls rely less upon human ability to detect an intrusion. A low level of sophistication (e.g. doors locked during the night) requires users to detect unauthorized personnel and activity during duty hours and the results of unauthorized activity

A-41
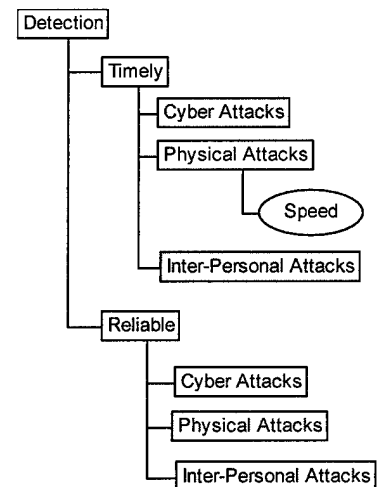
after the fact if the breach occurred during off-duty hours. A highly sophisticated system (e.g. electronic monitoring with 24-hour dedicated personnel) relies less upon the element of human recognition.

The time to physical intrusion detection is evaluated in hours, ranging from 0 to 72. Sophisticated systems will likely score well with very short time periods. Assuming a low-level control and an intrusion occurs immediately after personnel leave on Friday derived the worst-case (72 hours). The 72-hour period accounts for a two-day weekend, and gives the personnel until the end of the next duty day (Monday) to detect that an intrusion has taken place. Processes that take longer than the 72-hour period are assumed inadequate in providing timely detection.
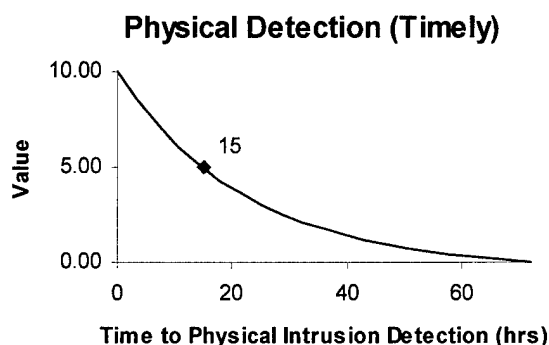
Figure A- 25: VF for Timely Detection of Physical Attacks

Timely (Inter-Personal Attacks)

Social Engineering is defined as "a deception technique utilized by hackers to derive information or data about a particular system or operation." [JCS IA, 1999:F-17] There are a number of methods to accomplish this, all of which focus on the lack of
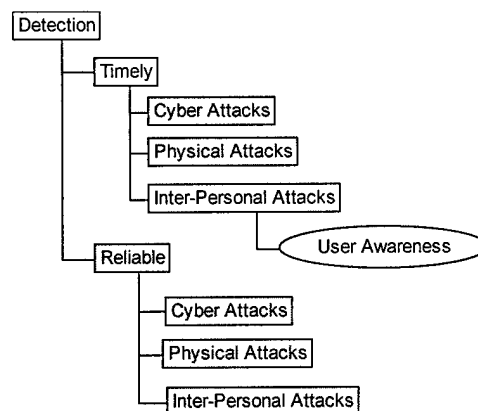
awareness or lack of training that authorized users possess (or both). Timely detection in this

context is assumed to rely upon the awareness of the users.

Regardless of the effectiveness of the associated training programs, the human is still the

weakest link in an information system. Job demands, complacency, and the time since the last

training session may result in a decreased awareness and an increased vulnerability to inter-

personal types of attacks. This measure assesses the percentage of users that are current to

evaluate the overall awareness of the user population. The meaning of 'current' is dependent

upon the time period specified by the organization, as well as the amount of training

commensurate with the level of access the user retains. For example, "Air Force military,

civilian, and contract personnel will receive information protection awareness-level training

within 60 days of permanent change of station/permanent change of assignment to a new

organization." [AFI 33-204, 1999:3] Additionally, although both a simple user and a system

administrator may be equally susceptible, the training provided to each individual should

emphasize the required awareness due to the different levels of authority.

Recency of Training
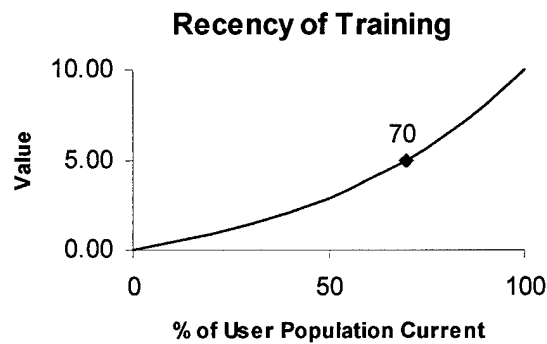
Figure A- 26: VF for User Awareness

Reliable (Cyber Attacks)

As mentioned in the Kendall's work, there are explicit tradeoffs between the false alarm rate and detection capability. [1999:17] The reliability of intrusion detection systems (IDS) determines how often they fail to detect a valid intrusion, and how often an anomalous event is construed as an intrusion (false alarms). High false alarm rates can consume valuable resources, and could potentially be used to an adversary's advantage. However, failing to detect a valid intrusion is assumed the more serious of the two possibilities. From a quality control perspective, these types of errors are defined as producer's risk (or Type I error) and consumer's risk (Type II errors), respectively. This concept is similar to the operating characteristic (OC) curve, which facilitates in the tradeoffs that must be made between these types of risks, as well as the overall reliability of the controls.
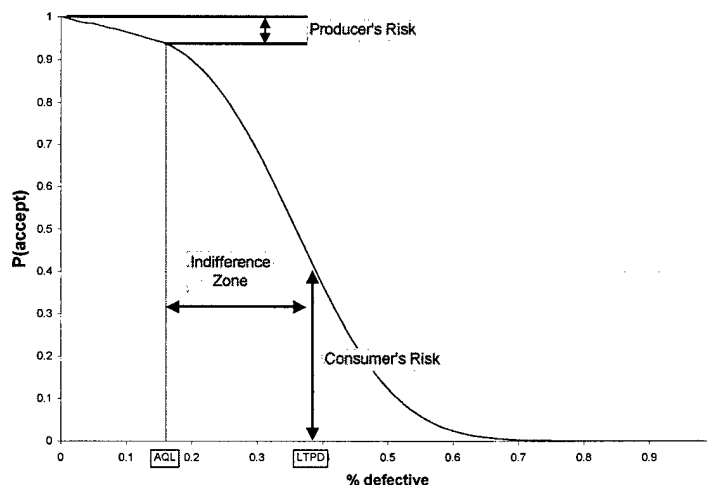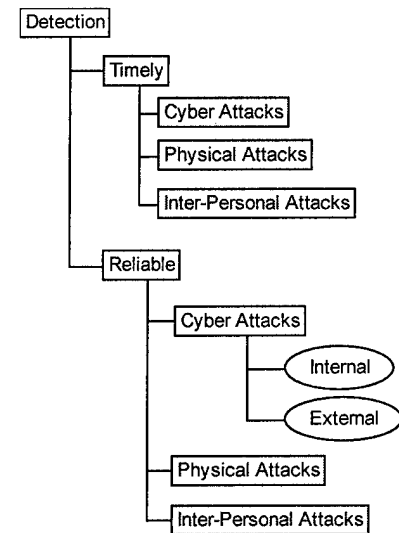
Figure A- 27: Operating Characteristic Curves [Monks, 1977:507]

Figure A- 27 illustrates the relationships between the producer and consumer risk, as well as the acceptable quality level (AQL) and the lot tolerance percent defective (LTPD) levels.

A-44

[Monks, 1977:507] The shape of this curve, and therefore the risk involved, is governed by the

sample size of inspected parts, which, in this context, is equated to the frequency of IDS updates.

Therefore, given that some capability is in place to detect cyber attacks—the exploitation

of system connectivity to gain unauthorized access—the 'sample size' used to improve the

power of the detection system can be seen as how frequently the system is updated to ensure

proper configuration. The configuration required, and the time between configurations, is

dependent upon the type of IDS. A notional evaluation measure is shown in Figure A- 28, where

the value provided is based upon how often IDS configuration is accomplished, thereby

influencing the reliability of their detection capability. The current range is from zero to 30 days,

denoting the time between IDS updates (e.g. policy updates, model training, or new attack

signatures). Zero days implies that it is automated and constantly updated, 30 days implies that

the system is checked on a monthly basis. Anything greater than 30 days is assumed outdated,

due to the rapid evolution of threat capabilities, and of little value to the decision-maker

concerning reliable detection of cyber attacks.
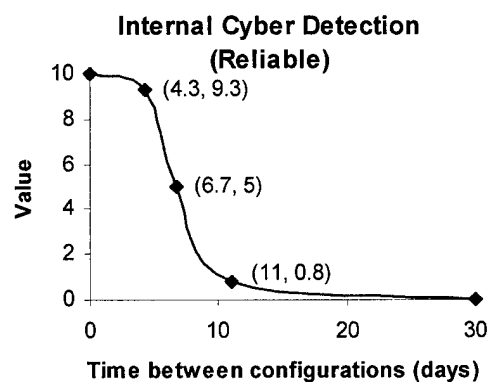
Figure A- 28: VF for Reliable Detection of Cyber Attacks

Figure A- 28 shows the evaluation function for assessing the reliability of external

attacks. The function for assessing the reliability of internal attack detection is identical and

based upon the same rationale. However, this assumes that some capability to detect

unauthorized behavior of an *authorized user* is in place.

Reliable (Physical Attacks)

This area evaluates the ability of an organization's

system and the level of user awareness to detect physical

attacks upon information systems' components or the

immediate area. This measure primarily appraises those

areas under the control of the organization—the

information system of interest. However, the connectivity

and interdependence of today's systems will eventually

Detection
— Timely
— Cyber Attacks
— Physical Attacks
— Inter-Personal Attacks
— Reliable
— Cyber Attacks
— Physical Attacks
— Physical Security
— Inter-Personal Attacks

require addressing a larger scope, to include the infrastructure supporting the IS.
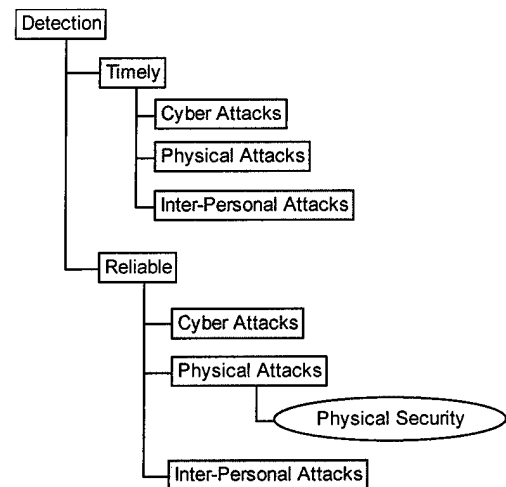
There are a number of means to detect physical attacks, to include premises alarm

systems, automated detection of unauthorized coupling of the immediate system (circuit and

power consumption analysis), breaks in connections resulting in temporary loss of capabilities,

etc. Personnel training (to increase awareness, and the probability of detection) to identify when

an attack is being perpetrated by an adversary (insider or outsider) by recognizing and reporting

behavior that may be unauthorized

Assuming some level of physical access control is in place, the reliability of the control's

detection capability is dependent upon how an intrusion is detected. Systems that require

authorized personnel to detect and notify (or fail to notify) the appropriate individuals to initiate

a reaction. The more sophisticated the control, the less reliant it is upon simple human

awareness to notice all attempted intrusions. More focused human awareness will increase the

probability of detection, and the integration of automated intrusion detection with a dedicated human element will increase the reliability even further.

For example, a door unlocked during duty hours and locked during off-duty hours (with no type of guardian) relies heavily upon the people near the door to detect entry of unauthorized personnel. If the intrusion occurred during off-duty hours, detection of the intrusion depends upon noticing any signs of forced entry (if any) upon return. The addition of dedicated personnel to control access can offer a more focused (and therefore more reliable) detection capability, assuming they have the ability to differentiate between authorized and unauthorized individuals. The reliability is negligible, however, during the times they are not present. More sophisticated physical controls, such as electronically controlled (and monitored) doors, may have the ability to control movement of personnel, and reliably detect intrusions (or attempted ones) through various means.

There are five levels for this measure which denote the varying level of human focus required for reliable detection of physical attacks: *Presence, Trained, Key Personnel (Duty-Hours), Key Personnel (Continuous)*, and *Automated.*

Detection of Physical Attacks (Reliable)

Value: Presence 2, Trained 4, KP-DH 7, KP-Cont. 8, Automated 10

Control Sophistication
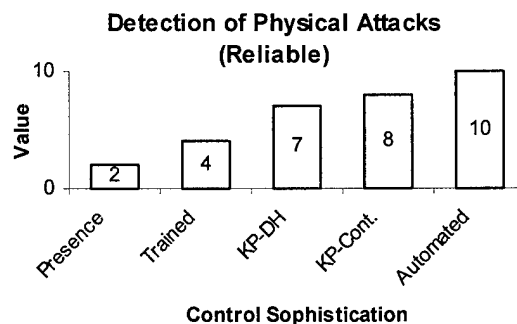
Figure A- 29: VF for Reliable Detection of Physical Attacks

Presence means detection capability is reliant upon the general awareness of authorized personnel, implies that no substantive physical controls are in place, except the presence of

authorized personnel. *Trained* indicates that the detection capability is primarily reliant upon the awareness of authorized personnel but is improved upon by appropriate levels of training and awareness. *Key Personnel (Duty-Hours)* implies that dedicated personnel are assigned to monitor points of access and other critical areas as determined by the organization, during regular duty hours only. This assumes that this measure is in addition to the requirement for the general population to remain aware of detecting physical attacks. *Key Personnel (Continuous)* means that dedicated personnel are assigned to monitoring points of access and other critical areas as determined by the organization on a continuous basis. *Automated* assumes that physical security controls are automatically enforced through electronic means and continuously monitor points of access and other critical areas as determined by the organization. This level also assumes that dedicated personnel are continuously monitoring all responses of the automated system.

Reliable-Inter-Personal Attacks

User Training evaluates the effectiveness of training programs designed to provide authorized users with the knowledge to recognize (detect) a potential inter-personal attack. Therefore, this area assesses the training incorporated into IA Strategies that focus on allowing users to detect an attempt to elicit information

that may be used for unauthorized activities. The levels include *Not Addressed, Mentioned, Discussed, Discussed-Illustrated,* and *Trained-Evaluated. Not Addressed* defines training that does not address or mention the dangers and methods of social engineering (SE) types of attacks. *Mentioned* classifies training that briefly mentions the dangers of SE attacks. *Discussed* means
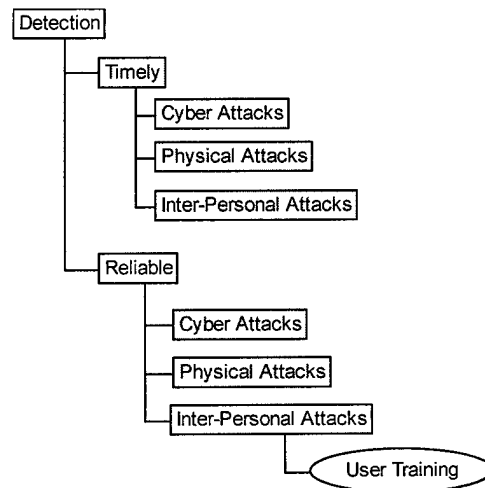
that SE attacks are described in detail. *Discussed-Illustrated* defines training that describes SE attacks in detail and portrays notional examples in order for the users to fully grasp the gravity and potential impact of SE types of attacks. *Trained-Evaluated* means that individuals are not only fully trained on this type of attack, but are periodically evaluated through random or standardized testing during the specified time period between recurring training.

Figure A- 30: VF for User Training

Reaction

Joint doctrine addresses the importance of response and restoration capabilities. [JP 3-13, 1998:III-10] In this analysis, these are grouped into the react objective, since both are dependent upon either attack detection, attack warning, or some other, perhaps natural, event that has caused or has the potential to cause some level of disruption.
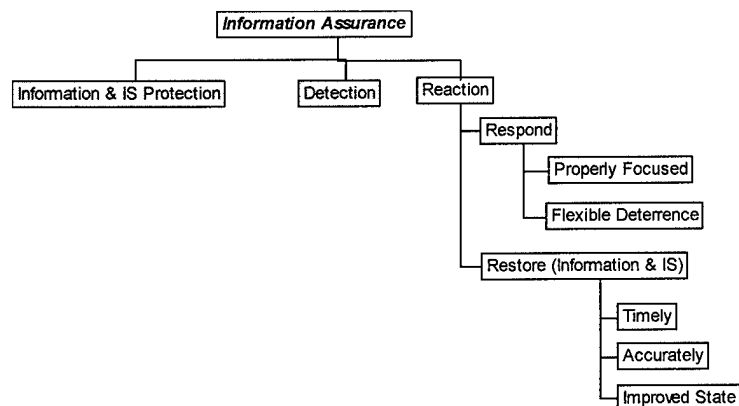
The requirements of reaction capabilities that support IA are generally composed of three objectives:

- Determine the appropriate response to an impending or detected attack by seeking an accurate identification of the attacker (or attackers) and their intent;

- Quickly respond to mitigate the effects of the attack by either halting the attack, letting the attack proceed in order to collect evidence, or taking retaliatory measures; and,

- Restore the information and information systems to at least the original state, but preferably, one that is improved to prevent similar attacks from occurring in the future.

For the purposes of this thesis, retaliatory measures will be limited to the pursuit of legal remedy. That is, for example, offensive information operations (e.g. computer attack), physical retaliation (e.g. bombing), or other means (e.g. embargo) are considered beyond the scope of this research. The overall objective of an effective reaction capability is to provide the organization with a properly focused response mechanism, and to restore the availability, confidentiality and integrity of information and information systems to their original or an improved state.

Respond (Properly Focused)

"Timely identification of actors and their intent is the cornerstone of effective and properly focused response, thereby linking the analytic results of the indicator and warning (I&W) process to appropriate decision makers." [JP 3-13, 1999:III-14] The *Properly Focused* objective assesses the ability to correctly identify the individuals involved, the vulnerabilities exploited and the motivation for the attack in order to form the most appropriate response against the attacker (or attackers). This process may be accomplished externally or internally.
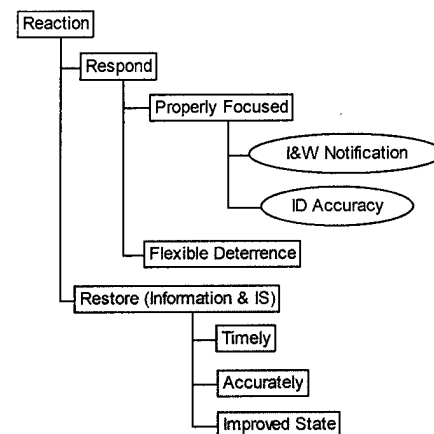
I&W Notification

External identification is based upon the level of support and communication that occurs between organizations concerning ongoing or increased potential for attacks. Joint doctrine emphasizes the value of "a reporting structure linked to intelligence, counterintelligence, law enforcement, policy makers, and the information systems community, both government and commercial." [JP 3-13, 1998:III-12] Many methods of notification and information sharing are available, and have varying levels of success. For this measure, it is assumed that a larger number of indications and warning sources available to system administrators and owners provide more identification ability than if they only acted alone. Five potential sources of I&W used for this measure are the intelligence community, law enforcement, policy makers, the government information systems community, and the commercial information systems community. It is further assumed that each source is of equal value, and that appropriate policies and procedures are in place to ensure adequate lines of communication are available when needed. The total number of sources available, assuming active involvement with each, provides the score for the IA strategy.
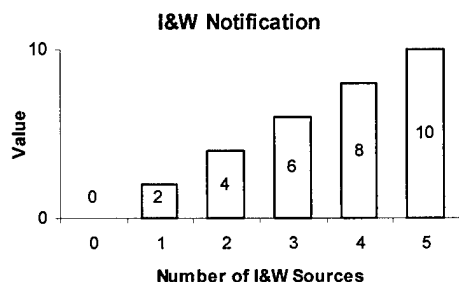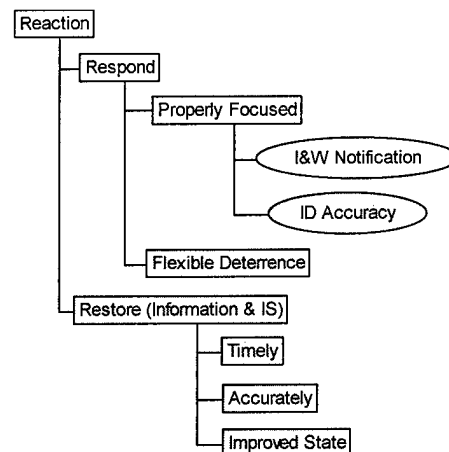
Figure A- 31: VF for I&W Notification

Identification (ID) Accuracy

Internal capabilities of identifying insider and outsider attacks are accomplished through a variety of means, depending upon the type of attack involved. Nonrepudiation is "assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data." [NSTISSI 4009, 1999:32] Although, this is generally accepted as a means of electronic verification, nonrepudiation could be extended to the physical world (e.g. the registered mail process).

Borrowing from DOD Instruction 5200.40, the attribution mode is a measure to "distinguish the degree of complexity of accountability required to establish authenticity and nonrepudiation." [1997:60] This is chosen as a constructed proxy to evaluate the organization's internal capability to correctly identify the threat parameters, and therefore facilitate a properly focused response. Four choices include *None, Rudimentary, Selected,* and *Comprehensive.*

- *None* means that no processing, transmission, storage, or data carries the ability to attribute them to users or processes.

- *Rudimentary* (Rud.) means the most basic processing, transmission, storage, or data carries the ability to attribute them to users or processes.

- *Selected* (Sel.) means some processing, transmission, storage, or data carries the ability to attribute them to users or processes.

- *Comprehensive* (Comp.) means all or almost all processing, transmission, storage, or data carries the ability to attribute them to users or processes. [DODI 5200.40, 1997:60]
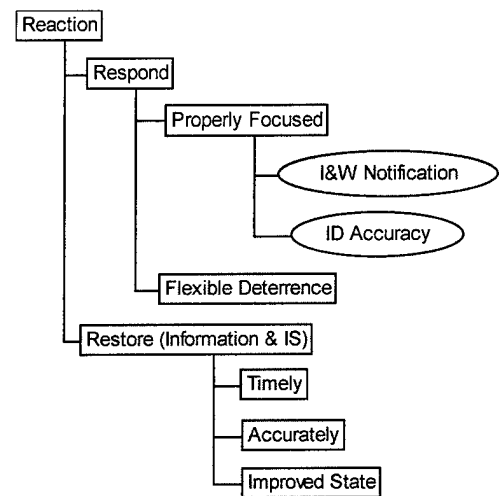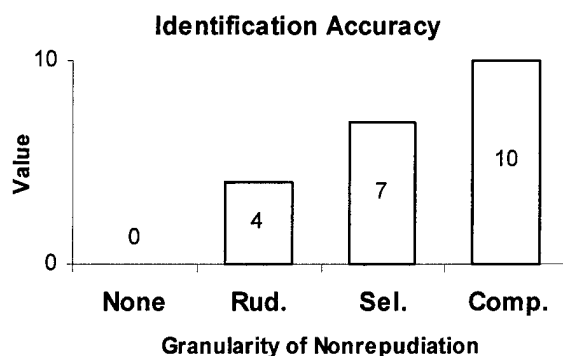
Figure A- 32: VF for ID Accuracy

Respond (Flexible Deterrence)

Once an attack is detected and those responsible have been identified, the organization must act to mitigate the risk posed to the organization. *Flexible Deterrence* entails taking the appropriate action at the appropriate time. In this case, the appropriate action entails either stopping the attack, or collecting evidence to facilitate legal action, or both. The appropriate time required to act upon threats depends upon the type of attack, the subsequent risks, and the capability of the organization.
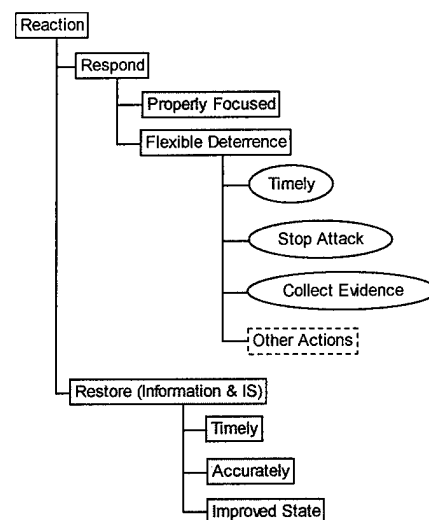
Timely

It is assumed that timely initiation of the appropriate response provides fewer potential gains to the adversary. Lower levels of authority required to initiate attack responses generally oppose the attack sooner. This evaluation measure assesses the policy and procedures, in place or recommended, that provides for response initiation. It is assumed that the higher level of authority required to begin mitigating procedures, the longer the adversary will have to cause damage to the information and information systems. The level of authority required serves as a

proxy for the timeliness of initiating deterrence, and the types of authority provide a constructed scale.

Timely Initiation of Deterrent Options
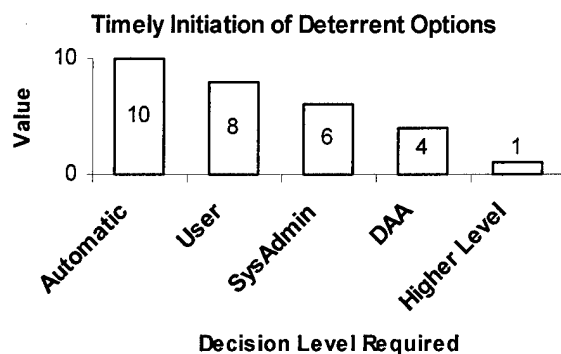
Figure A- 33: VF for Timely Deterrence

There are five levels for this measure: *Automated, User, SysAdmin (Systems Administrator), DAA,* and *Higher Level. Automated* means that attack response does not rely upon any human intervention in order to initiate the attack response. Note that this may be the timeliest method, but an adversary seeking to consume system resources may also exploit it. *User* means that an authorized user can initiate the response. *SysAdmin* is defined as the lowest authority to initiate the attack response is owned by the System Administrator. *DAA* will be that the lowest authority to initiate the attack response is the individual that assumes responsibility for the system—the designated approval authority. Finally, *Higher Level* indicates that the next level of authority past the DAA must approve the initiation of the attack response.

To evaluate a variety of attack response options, this measure may be broken down into finer levels of detail. Evaluation of how each type of attack response is initiated, and then weighted by an estimate of the probability of each type of attack occurring would yield an overall (average) score for the organization's timely deterrence.

Stop Attack

Tradeoffs exist between terminating an attack and allowing it to progress, facilitating the collection of evidence for law enforcement officials to then take action. Assuming that the risk posed by an attack is too great to allow for evidence collection, the ability to stop an ongoing attack is vital. However, the method of terminating an attack may adversely affect the availability of data or performance of the system. It also varies with the types of attacks. For these reasons, a categorical measure is developed to assess the general capability of an organization to stop an attack. The three categories are *No Capability*, *Manual*, and *Automatic*. Similar to other evaluation measures, the capability to stop different types of attacks may be evaluated individually, and then weights may be used as a proxy for the probability of each type of attack occurring.
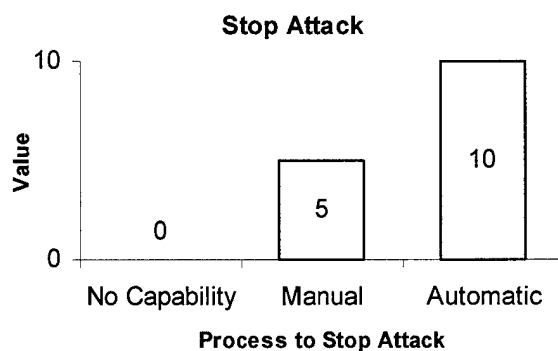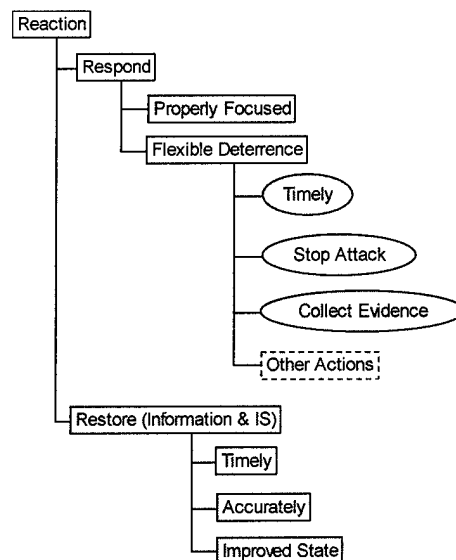
Figure A- 34: VF for Stop Attack

Collect Evidence

The *Collect Evidence* attribute measures the organization's ability to ensure that threatening actors' (both internal and external) identities, intentions, methods (i.e. identification of the vulnerabilities that were exploited) and motivations are brought forth to facilitate the legal actions that may be taken.

Increasing the level of complexity typically increases the amount and types of data collected, offering a better chance to apprehend and prosecute the offender(s). Note that this measure is not strictly limited to cyber attacks. For example, where audit logs may serve as repositories for threat activity, cameras serve as auditing tools for physical activity. Essentially, the capability to allow attacks to proceed facilitates the vulnerability and attack origin identification, which provides value to the DM, regardless of means. The question remains as to the level of risk associated with allowing a threat to continue its activities. For this measure, a categorical assessment of evidence collection capability includes four levels: *No Capability*, *System-Medium*, *System-Low*, and *Benign*.

No Capability means that the IA strategy has no capability to divert or control a threat once detection occurs. *System-Medium* means that the capability exists to contain the threat within the system, but the risk of allowing further penetration is assessed as medium due to other controls and policies in place. *System-Low* means that the capability exists to contain the threat within the system, and the risk is perceived as low due to the level of controls and policies in place (e.g. a strong defense in depth exists). *Benign* means that the capability exists to reroute
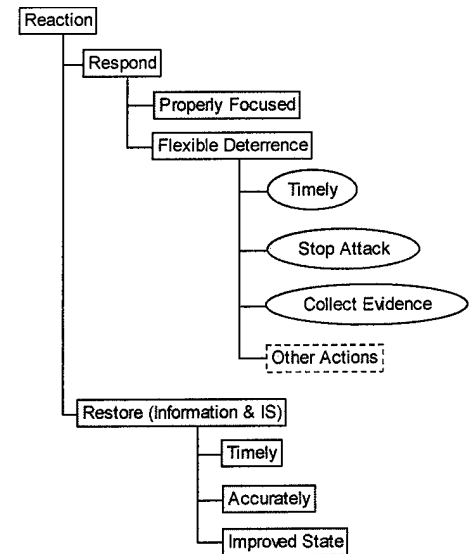
the threat to a benign environment, allowing for collection of evidence, with no additional risk posed to the organization.
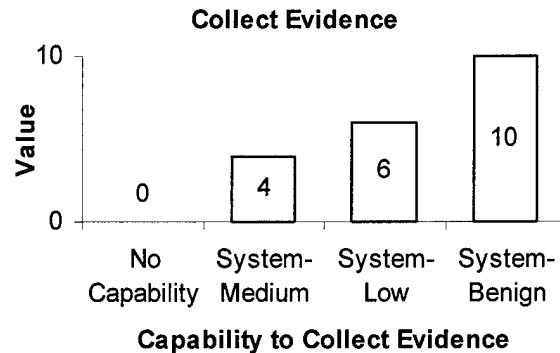
Collect Evidence

Figure A- 35: VF for Collect Evidence

Other Actions

As discussed earlier, this thesis does not account for deterrent options beyond the pursuit of legal means. This area lends itself to future analysis.
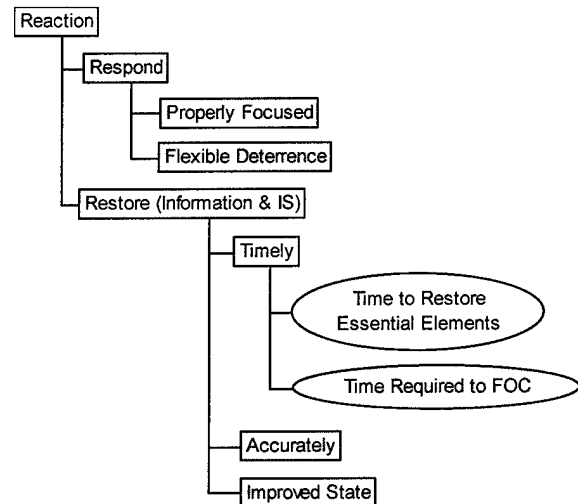
Restore

The overall objective of restoration is to minimize the disruption associated with attacks or natural events, by restoring the availability, confidentiality, and integrity of the information and the information systems. The ability of an organization to restore information and information systems "relies upon established procedures and mechanisms for prioritized restoration of essential functions." [JP 3-13, 1998:III-12] The time to restore depends upon the amount of damage done. The damage due to a logic bomb, an electronic mail bomb, or a pipe bomb may vary, and the means to restore the damage are obviously different. Therefore, this area evaluates the robustness of the restoration capability within an IA strategy, with the focus on three areas:

- The speed at which prioritized services and information sources are restored;

- The amount of accuracy or information that may be lost as a result of the restoration process; and,

- The ability to bring the IS to an improved state, reducing the probability of success given an identical attack in the future.

Time to Restore Essential Elements

There are a number of mechanisms to restore information and IS services, to include technical and non-technical means. These mechanisms, however, may vary in the time required to complete the restoration process. This measure evaluates the time required to restore essential elements, which may be comprised of information sources, IS components, or services provided by the IS. Determining essential services is organization-specific. However, in this context, essential is defined as an element that sustains the organization's ability to accomplish its stated objectives. If an essential element is not available, then the organization is assumed unable to perform the related mission.

To implement this measure, an evaluation function must be developed for each element identified as essential to the organization. The maximum time for the range of each measure is determined by the maximum amount of time that the element may be unavailable (or compromised) while still allowing the organization to perform the mission associated with the element. Prioritization between these essential elements is then accomplished through the proper weighting of each evaluation measure.

A-58
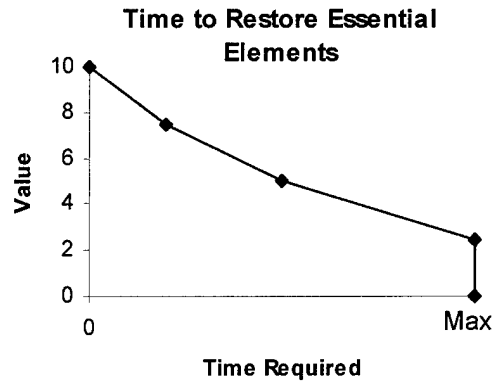
Figure A- 36: VF for Time to Restore Essential Elements

A time of 0 would indicate that the restoration process is fully automated. An alternative

would be to use the best restoration time that has been demonstrated by similar organizations.

The maximum time is determined by establishing organization-specific, operationally acceptable

times. It is assumed that simply meeting the maximum criteria attains some value to the

decision-maker.

Time Required to Fully Operational Capability (FOC)

Eventually, the system and its information must return
to its original state, becoming fully operationally capable.
The intended use of the system plays a major role in the
maximum allowable time that the system is not FOC. FOC
implies that all elements, essential and otherwise, are
functioning properly.
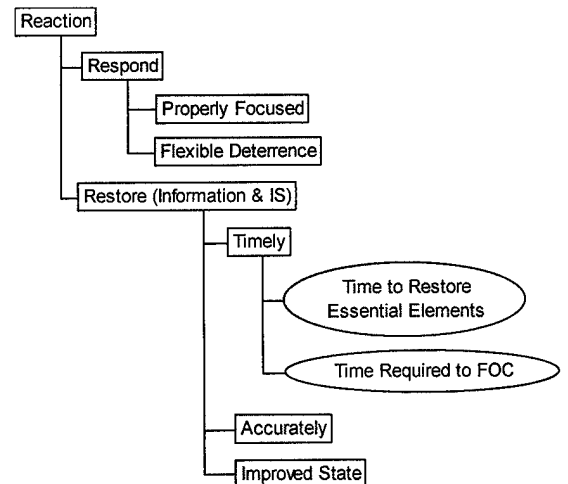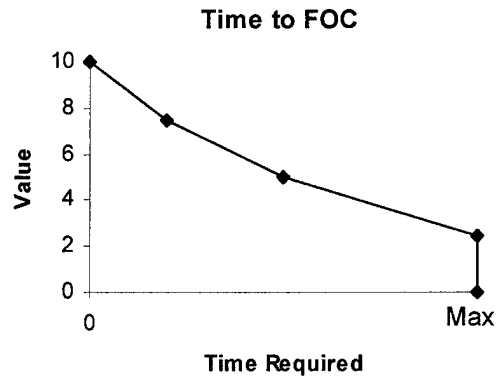
Figure A- 37: VF for Time Required to Full Operational Capability

This measure is assessed in the same manner as the time to restore essential services, with the exception that the system cannot be in a degraded state of operation.

Restoration Accuracy

In addition to the time required for restoration, the accuracy of the restoration process is critical to maintaining the intended functionality, as well as minimizing the amount of information loss. This measure
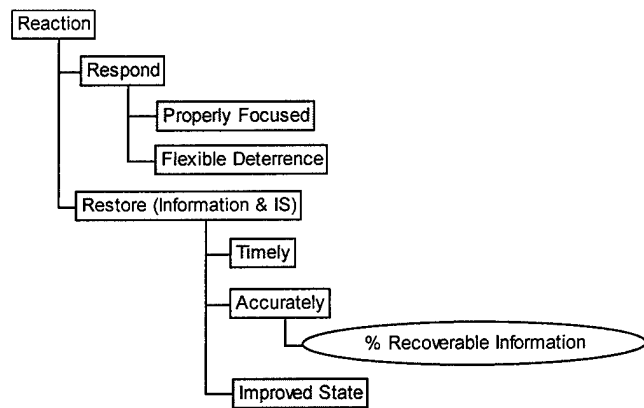
attempts to capture both areas through an estimate of the IA strategy's capability to restore the information. Underlying issues include the methods of backing up information (particularly how much and how often) and how and where the archive is stored.

Restoration Accuracy
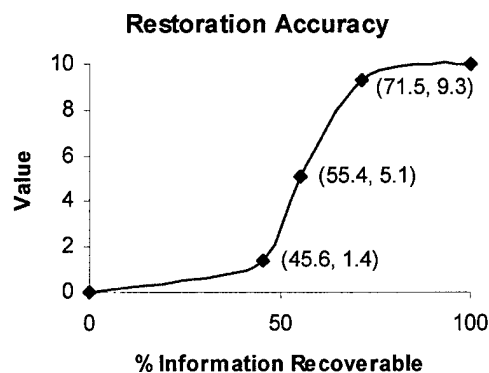
Figure A- 38: VF for Restoration Accuracy

The methods and frequency of backup capabilities vary widely. In addition, considerations must be made regarding the value of information over time. For example, if a system fails and the backup information is outdated beyond acceptable use, the accuracy is assumed negligible. Expert assessments, historical data, or testing the system (where possible) should facilitate the estimation of this measure. The shape of the curve assumes that there is some threshold value (%) that must be met in order for the organization to continue an operationally acceptable level based upon information restored from backup data.

Improved State

In order to provide the most value to the DM, the restoration process must also prevent further attacks similar in nature by returning the system and information to an improved state from which it began. This may be accomplished by eliminating the exploited vulnerabilities, either within the physical or cyber realms.

Resource Inventory

"A key step in capability restoration is to inventory systems resources to help identify surreptitious adversary implants." [JP 3-13, 1998:III-13] From this, using the percentage of applicable items that have been inventoried offers a direct and natural measure of the physical changes required improving the system state.
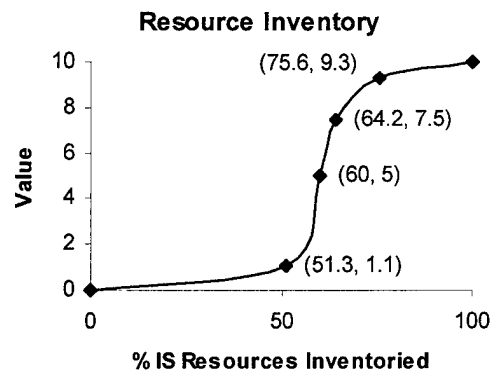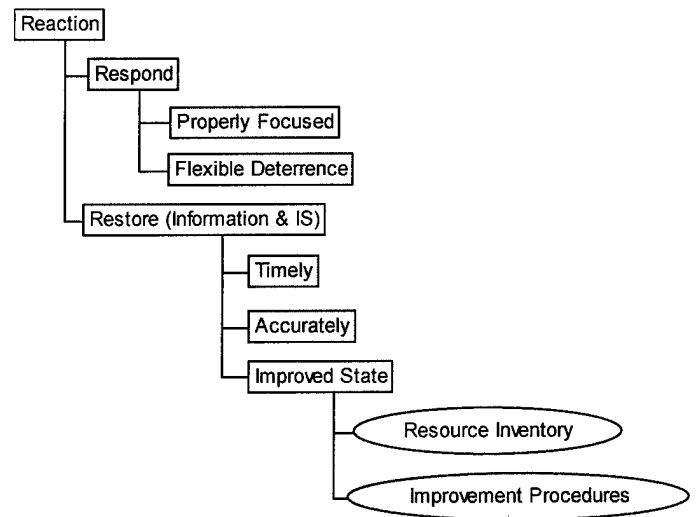

Figure A- 39: VF for Resource Inventory

Note that there is a maximum uncertainty associated with only having 50% of the items inventoried, hence a low score is assigned when 50% or less of the system has been inventoried. A strategy is evaluated by measuring the percentage of components that have been inventoried within an operationally acceptable time period. The resolution to which these components are identified (i.e. computer versus internal hard-drive) are likely system specific, and will require time and cost tradeoffs.

Improvement Procedures

"Post-attack analysis provides information about vulnerabilities exploited and leads to security improvements. Audit trails such as automated recording of specific attack techniques during the incident can provide information required for analysis."
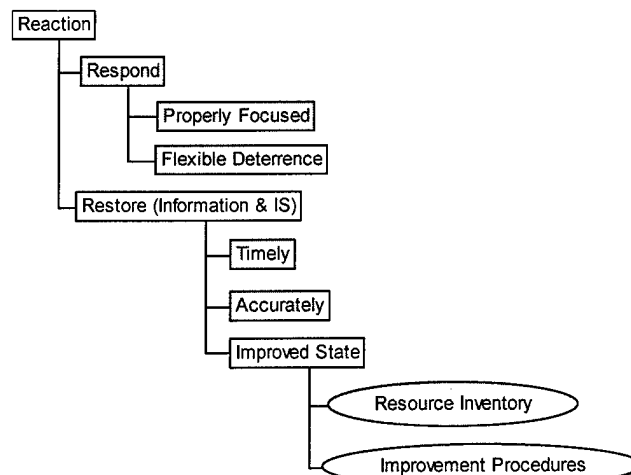

[JP 3-13, 1998:III-13] This measure assesses the procedures that are in place or recommended as part of an IA strategy that yield potential improvements to the system after post-attack restoration. It is assumed that the effectiveness of these procedures are dependent upon the time and number of people dedicated to analysis efforts, the tools available, and the expertise of the analysts. Therefore, the existence of such procedures would provide value to the DM, and the effectiveness would involve tradeoffs against resource costs. This measure simply captures the existence (or lack thereof) of an improvement process, the importance of which is emphasized in Joint Doctrine.
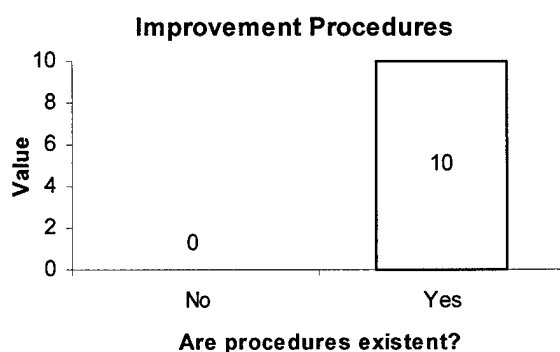
Figure A- 40: VF for Improvement Procedures

Summary of IA Hierarchy

Figure A- 41 illustrates the complete value hierarchy developed to evaluate the level of Information Assurance provided by a given strategy. Unfortunately, these strategies typically come with potential reductions in operational capability and costs associated with information technology and support. The next logical step, then, is to address the changes that may occur in operational capability.
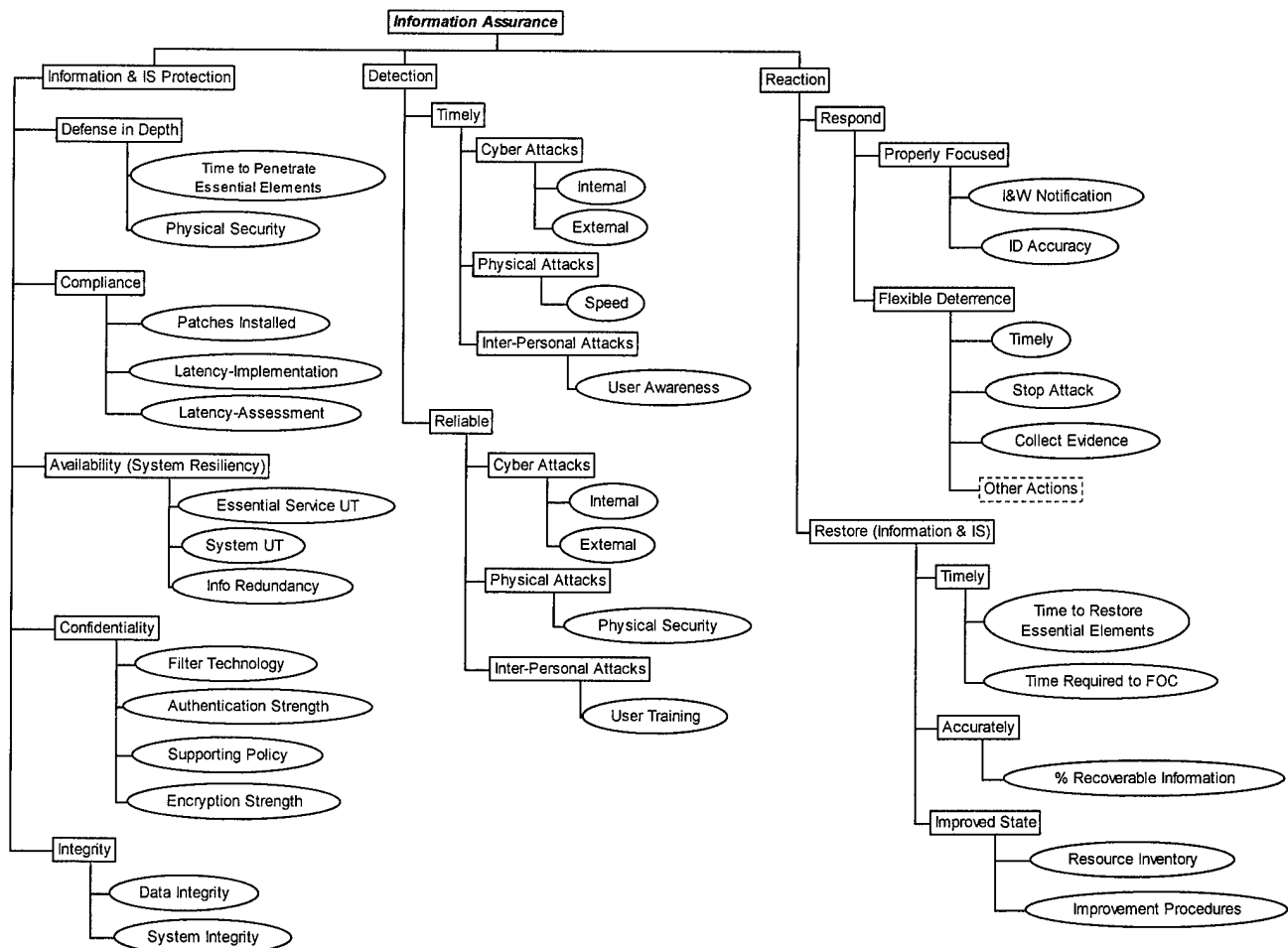

Figure A- 41: Complete IA Value Hierarchy

Operational Capability

       Increasingly complex information systems are being integrated into traditional warfighting disciplines such as mobility; logistics; and command, control, communications, computers, and intelligence (C4I). Many of these systems are designed and employed with inherent vulnerabilities that are, in many cases, the unavoidable consequences of enhanced functionality, interoperability, efficiency, and convenience to users. [JP 3-13, 1998:I-11]

The *Operational Capability* hierarchy accounts for the changes (good and bad) in

functionality, interoperability, efficiency and convenience that result from implementing an IA

strategy. Additionally, the IA goals of DARPA's Next Generation Information Infrastructure

(NGII) are to develop security and survivability solutions that "reduce vulnerability and allow

increased interoperability and functionality." [JCS IA, 1999:A-66] These potentially conflicting

goals provide an ideal setting for the VFT methodology. This hierarchy attempts to measure

these effects, and assumes that the DM wants to minimize any adverse impact upon the existent

system at a reasonable level of information assurance.
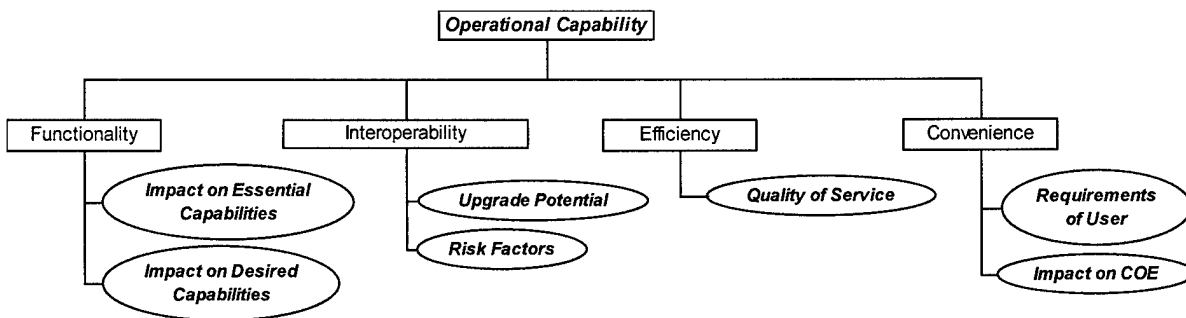
Figure A- 42: Value Hierarchy for Operational Capability

Functionality

       The objective of *Functionality* is to maximize the

number of services or functions offered to the users. However,

some IA strategies may result in a loss of previously enjoyed

functionality. Two constructed measures have been developed to directly quantify the

A-65
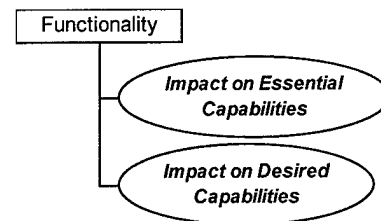
subsequent functionality of the IS—*Impact on Essential Capabilities* and *Impact on Desired Capabilities*. *Essential* capabilities are those services that an organization currently relies heavily upon to accomplish their stated mission. If these services are no longer made available, it is assumed that other means must be found to enable the organization to accomplish mission objectives. Desired capabilities are defined as those capabilities that offer enhanced mission effectiveness, but are not required to perform their stated objectives.

Impact on Essential Capabilities

As an initial cut at a measure, this evaluation measure assesses any impact (good or bad) an IA Strategy may have upon services and information currently accessible to authorized users. This focuses only on those services (or supporting services) that are of value to the DM or the majority of authorized users. This measure assumes that each service of interest is equal in value; however, weights, if known, could of course be used. Therefore, if one service is gained and another is lost, the net change in services is zero. Service in this context will be defined as a method of transferring or access to information. For example, the capability to access to a maintenance database remotely and the capability to move information from that database (i.e. via file transfer protocol, or ftp) are each considered services for the purpose of this measure.

A-66

**Impact on Essential Capabilities**
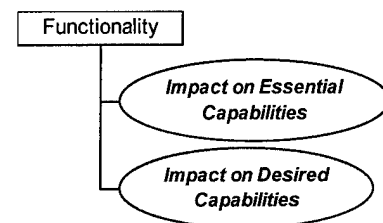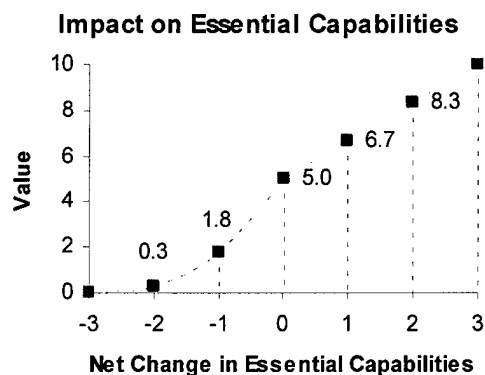
Figure A- 43: VF for Impact on Essential Capabilities

This evaluation measure assumes that if three or more (net) essential services are lost, this strategy (or the countermeasure contributing to the loss) is of no value in the context of accessibility.

Impact on Desired Capabilities

This measure is implemented similarly to the *Impact on Essential Capabilities* evaluation measure, with the exception of the types of services and capabilities assessed.

Note that the shape of the evaluation function will likely differ from that of the essential capability evaluation function.

Impact on Desired Capabilities
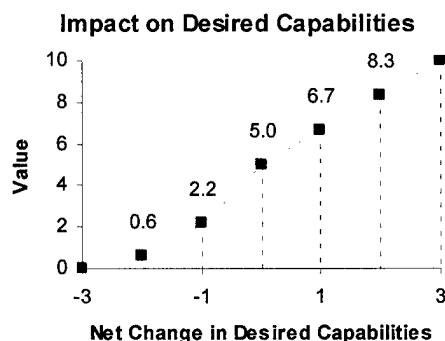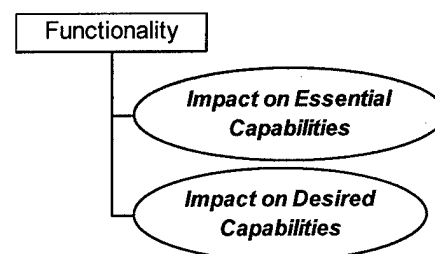
Figure A- 44: VF for Net Change in Desired Services

A-67

Interoperability

Systems that are interoperable and can be easily integrated with current and future systems provide immediate and cost-effective value to the DM. *Interoperability* assesses two areas with respect to the changes an information system may undergo during IA strategy implementation. These measures focus on the potential for future upgrades and additional risk that may be incurred by using state of the art technology or promising, yet unproven, procedures.

<u>*Upgrade Potential*</u>

The types of components that comprise the IA strategy may have an impact on future maintenance and/or possibility for upgrades. One-of-a-kind, system-specific components are not only costly, but they may not be capable of incorporating or inter-operating with future upgrades. Component type will serve as a natural proxy for upgrade potential.
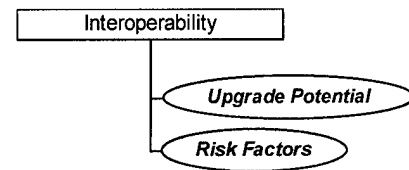
Commercial-off-the-shelf (COTS) products are (typically) the easiest types of components to obtain, maintain, and upgrade. The integration of industry standards into COTS contributes to fewer interoperability problems and allows "immediate leveraging of the existing IA capabilities afforded by commercial technology." [JCS IA, 1999:4-8]

Government-off-the-shelf (GOTS) products are those that have been developed and are owned by the government and used explicitly for government purposes. Although GOTS products may be better suited to performing government objectives with a greater level of trust and assurance, "traditional GOTS-based implementations cannot keep pace with fast-paced change in commercial technology." [JCS IA, 1999:4-8]

A third, potential source of countermeasures that may be included within an IA strategy are Non-Developmental Items (NDI). These items are defined as

A-68

"… any item that is available in the commercial marketplace; any previously developed item that is in use by a Department or Agency of the United States, a State or local government, or a foreign government with which the United States has a mutual defense cooperation agreement; any item described above, that requires only minor modifications in order to meet the requirements of the procuring Agency; or any item that is currently being produced that does not meet the requirements of definitions above, solely because the item is not yet in use or is not yet available in the commercial market place. [DODI 5200.40, 1997:12]

For the purposes of this study, NDI's are broken down into two categories—NDI-Existing and NDI-Future—which represent those in the marketplace and those not yet available respectively.

A final category is the 'one of a kind' system (hardware or software) that is developed solely for the information system of interest. This is assumed to be the least-preferred category, due to the developmental and supporting costs incurred, as well as the potential for interfering with future interoperability due to its uniqueness. These categories are shown in a proposed order of preference in Figure A- 45.

Upgrade Potential

Component Source	Value
COTS	10
NDI-Existing	8
GOTS	7
NDI-Future	3
One of a Kind	0
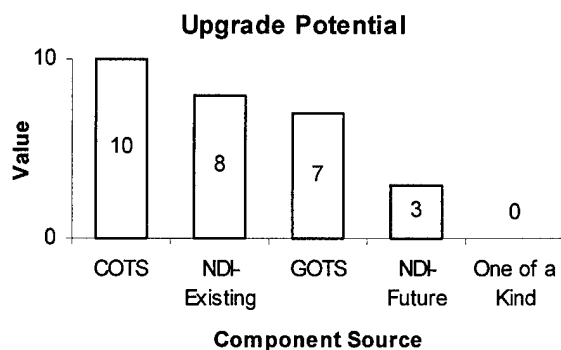
Figure A- 45: VF for Upgrade Potential

Note that this measure lends itself to comparisons between single components. However, in order to score an overall strategy that may include a number of each types of component, the following approach may be used. First, the scores for each category of component source must be determined by the decision-maker. Once these are established, the average score of all

components may be used as the overall value of the IA strategy with respect to *Upgrade Potential*. For example, if a strategy called for two COTS, one GOTS, and three NDI-Future components, the overall score would be (10+10+7+3)/4 = 7.5 on a scale from zero to 10. This assumes that each component is independent of each other.
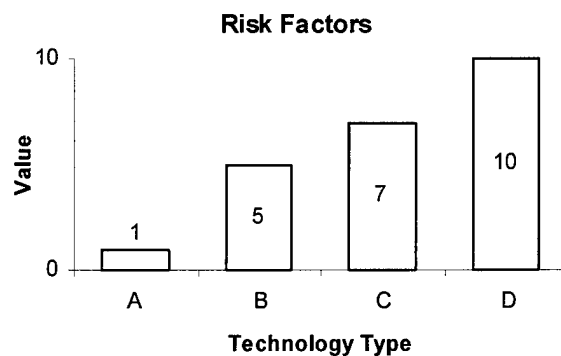
Risk Factors

This measure evaluates the additional risk that may be associated with implementation of certain types of countermeasures within a strategy. This risk applies to the likelihood of new vulnerabilities being introduced into the system, to include the possibility of incompatibility. It is assumed that the level of this risk is predicated upon the maturity of the technology, which will serve as a constructed proxy for these types of risk. The categorical scale shown in Table A-7 describes the levels of technological maturity evaluated.

Table A- 7: Description of Risk Categories

Risk Category	Description
A	Never been operationally used in any information system
B	Never been used on the type of system specific to the organization
C	Has been used on the type of system specific to the organization, but not with the given configuration
D	Has been used on a system-configuration similar to that of the organization's system

As seen in the *Upgrade Potential* evaluation measure, an overall assessment of multiple types of components must either be averaged, or expert opinion may score the strategy using the worst case or the value of critical or major components.

Figure A- 46: VF for Risk Factors

Efficiency

The quality of service measure will serve as a constructed proxy for the effects IA

strategy implementation will have upon the efficiency of the information system.

<u>*Quality of Service*</u>

The Next Generation Internet (NGI) initiative is a multi-sector effort that, "together with

other investment sectors, will create the foundation for the networks of the 21st century, setting

the stage for networks that are much more powerful and versatile than the current Internet."

[NGI, 1998:1] Within this effort, one of the major goals is the facilitate "the delivery of end-to-

end ensured Quality of Service (QoS)." This strategy will allow users to tailor the way they use

technologies according to their requirements. Negotiation of "application-specific tradeoffs

among such parameters as bandwidth, latency, precision, and reliability in order to obtain

predictable performance at a known quality level" will be possible. [NGI, 1998:10] Currently,

the QoS that an information system provides is predominantly system-specific, based upon the

architecture and operating system employed, and is dependent upon the workload at any given

time. Therefore, the degradation of QoS due to the addition of components (countermeasures)

may not be perceived consistently throughout the IS, if at all. For these reasons, a categorical

assessment of the impact that an IA Strategy may have upon information system's QoS is offered.

This measure includes five categories: *Improved, None, Slight, Substantial,* and *Unacceptable. Improved* means that a majority of the users perceives an improvement in the QoS of network performance and services. *None* implies that any user, regardless of the overall demand upon the system, cannot perceive any difference in the quality of service. *Slight* indicates that a few to all users (10% to 100%) will notice a reduction in network performance, regardless of the overall demand upon the system. *Substantial* means that all users will notice a reduction in network performance (QoS), particularly if there is heavy demand upon the system, resulting in decreased capability to employ the IS and its services. *Unacceptable* signifies that implementation of the IA Strategy (or perhaps one of its components) will result in dramatic reductions in the QoS, resulting in severely degraded or ineffective capability to employ the IS and its services.
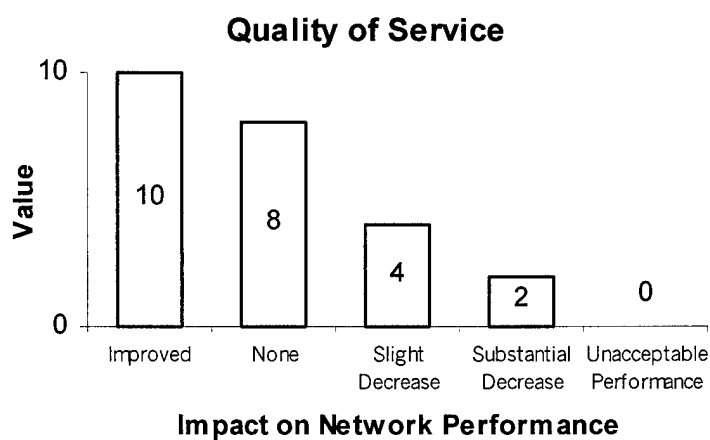
Quality of Service

Figure A- 47: VF for Quality of Service

Convenience

The objective of *Convenience* assesses the impact upon the human interfaces with the information system of interest. Interactions evaluated includes the requirements a user must fulfill in order to gain authorized access, and the demands placed upon the user to employ and benefit from the IS once access is gained.

<u>*Requirements of User*</u>

This measure evaluates the requirements placed upon the user in order for them to gain (authorized) access to the IS and the applicable information. This can include the requirements to physically access the system as well as the requirements for identification and authentication. Due to the diverse I&A methods, numerous physical access control techniques, and organization-specific security policies, a simple time scale is developed to evaluate the average amount of time it takes a user to log-on to the system. The time starts when the (authorized) user gets to the outermost protective layer of the facility housing the IS and ends when the user has access. It is assumed that the outermost layer may consist of some physical security measure that is intended to prevent entry of unauthorized individuals into the facility housing the IS. Therefore, if the outer doors to a facility are unlocked (during the day, for example), then the time would start either when the user comes to another control or the computer itself.

The minimum and maximum times provide the range. Inclusion of the current state is also required to assess degradations as well as improvements. This measure is a proxy for requirements placed upon the user, as well as the level of difficulty. For example, requiring the user to keep a token on their person, implementing multiple physical and virtual security controls
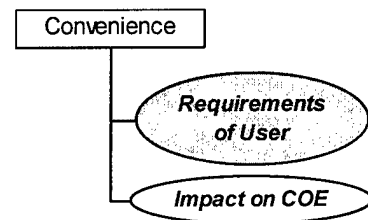
and other tedious and time consuming process may buy more security at the expense of

preventing users from employing the IS and its information in an operationally effective, or

timely, manner. A notional evaluation function is shown in Figure A- 48.

Impact on User Requirements
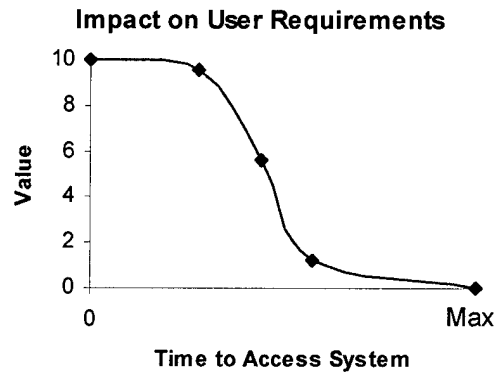
Figure A- 48: VF for Impact on User Requirements

The S-shape denotes that up to some threshold value, there is little change in the score.

However, once the time is beyond the threshold value, the score decreases dramatically. The

range goes from zero to some maximum time limit that would be considered unacceptable and of

little value.

Impact on Common Operating Environment

The Common Operating Environment (COE) attempts to…

"Provide a familiar look, touch, sound, and feel to the commander, no matter where the commander is deployed. Information presentation and command, control, computers and intelligence system interfaces are maintained consistently from platform to platform, enabling the commander to focus attention on the crisis at hand." [JP 1-02, 1999:91]
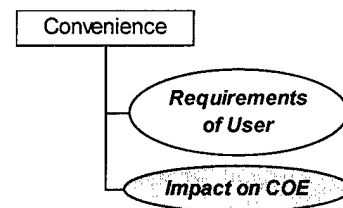
From this, it is important to evaluate the impact that a CM may have upon the COE of the

system of interest. This measure has three levels: *Negative Impact, No Impact*, and *Positive*

Impact.
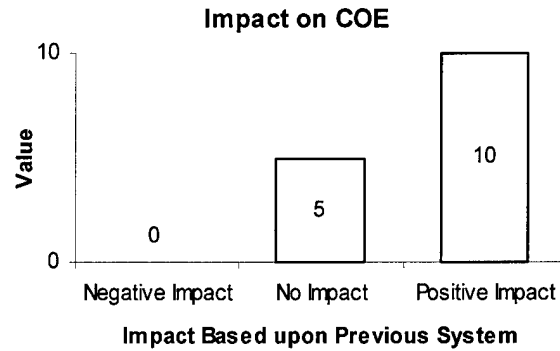
Figure A- 49: VF for Impact on COE

Negative Impact signifies that a number of noticeable changes have occurred that results in a discernibly different human-system interface requiring substantial training before users can effectively employ the system. *No Impact* implies that implementation of an IA Strategy and its countermeasures are transparent to the user ('Commander'). This assumes that the current system is appropriately designed. *Positive Impact* means that the IA Strategy implemented some level of change to the human-system interface that facilitates use with a minimum amount of training and orientation.

Consideration of Resource Costs

"Technology that affects an adversary's information and information systems and protects and defends friendly information and information systems will be pursued at every opportunity to ensure the greatest return on investment." [JP 3-13, 1998:I-5] This statement emphasizes the fact that, in an environment of shrinking budgets, costs associated with the IT to fulfill IA requirements must be considered. However, there are additional costs associated with some of these technologies. Figure A- 50 illustrates the cost hierarchy addressed in this research.
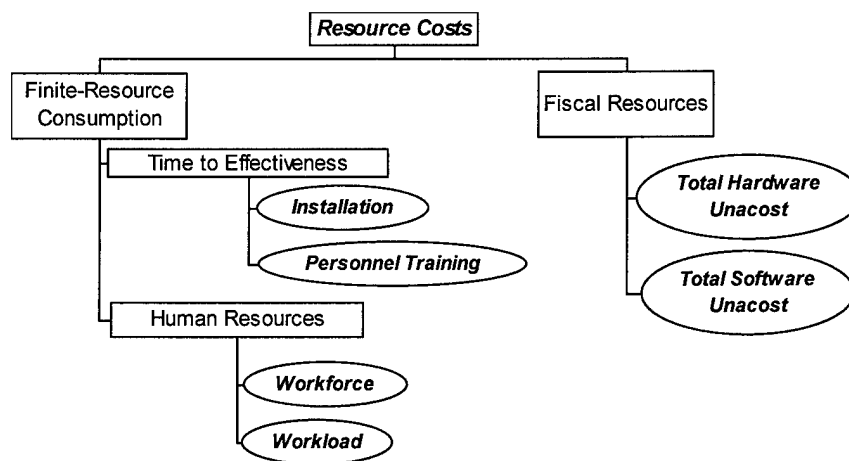
Figure A- 50 – Resource Cost Hierarchy

For the purpose of this study, IA costs are grouped into two categories: *Finite-Resource Consumption* and *Fiscal Resources*. *Finite-Resource Consumption* accounts for the tangible, direct costs incurred in time and people from procuring and/or implementing an IA strategy. The *Fiscal Resources* accounts for the dollar costs associated with procuring and/or implementing an IA strategy. It is important to note that for the evaluation of costs, a high value implies a low-cost alternative. Therefore, on a scale from 0 to 10, 0 is least preferred (high cost) and 10 is preferred (low or no cost). This methodology only accounts for the total costs in time, people, and money required to procure and implement an IA strategy. Opportunity costs (in dollars), as well as any sunk costs of the legacy system, are not considered. Additionally, salvage value of

items being replaced is not directly addressed, but may be accounted for given the appropriate accounting procedures. However, the salvage value of IT items is often relatively low.

Finite Resource Consumption-Time to Countermeasure Effectiveness

The time required in order for a particular countermeasure (CM) within an IA strategy to become effective is a function of two things—how long it takes to install the CM, and how long it takes the appropriate personnel to get any required training. A CM that is easy to install and requires no training for it to be effective incurs less "cost" in time than a CM that is difficult and time consuming to install and also requires significant training time before it becomes operationally effective. The rationale behind the importance of this measure is derived from Figure A- 9.
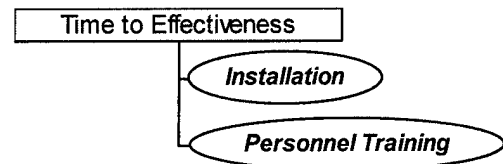
As time progresses, the system vulnerability to older types of attacks typically decreases as improvements are made to the information system. Although Kendall's research was focused primarily on (virtual) intrusion detection, the concept may apply to any type of countermeasure. The longer a CM takes to implement, the longer the system remains vulnerable. It is assumed that the DM prefers to minimize the time that the organization's information and information system are exposed to vulnerabilities identified, thus 'shrinking' the length of Figure A- 9.
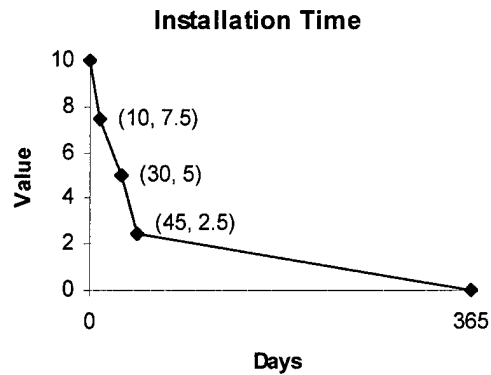
<u>*Installation Time*</u>

Installation Time is assumed to range from seconds (for automated updates of software) to months (for acquisition and emplacement of hardware). The upper limit may be subject to change, depending upon the nature of the vulnerability or the intended use of the IS and sensitivity of the information. The notional evaluation function shown below uses a range from 0 to 365 days,
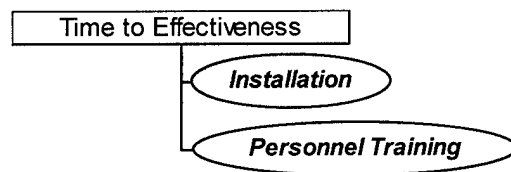
with a mid-value point at 30 days, and a ¼-value point at 45 days. Note that the actual score will

be determined by the total time required to install all elements within an IA strategy, based upon

a reasonable schedule (which may allow installations occurring in parallel).

Installation Time

Figure A- 51: VF for Installation Time

Personnel Training

Personnel Training is measured in a similar

fashion to *Installation Time*. This measure emphasizes

the need for efficient training programs, so that any CM employed can afford the organization

the intended level of assurance in a minimum amount of time. Note that the funded elements of

training costs (initial and recurring) will be included in the associated hardware or software costs

corresponding to the CM. The strategy will be scored on the number of days that must be

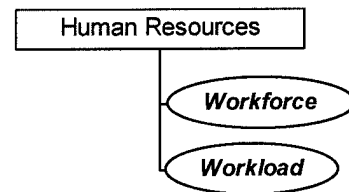scheduled to properly train the personnel in effective implementation.
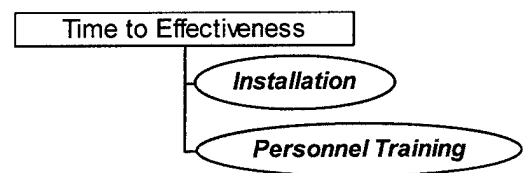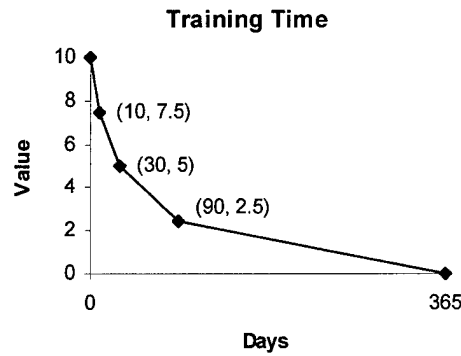
Figure A- 52: Training Time

*Finite Resource Consumption-Human Resources*

The *Human Resources* objective assesses the costs incurred

with respect to personnel. This is accomplished by two measures:

Additional Personnel and *Additional Workload*. This initial effort does not yet account for the

salary costs of different people (i.e. manager vs. administrative assistant) but focuses on the

relative change in workforce of the organization.

Workforce

The measure *Workforce* evaluates the percent increase in personnel that would be

required to carry out an IA strategy. This measure assumes that the requirement of additional

personnel is not preferred simply due to the hiring, training, and salary costs. The percentage

allows for a measure that is relative to the original size of the organization. For example, a 10%

increase would mean one person to an organization of 10, and 10 people to an organization of

100. For the purposes of this research, it is assumed that the marginal effect of either situation is

the same.

Workforce
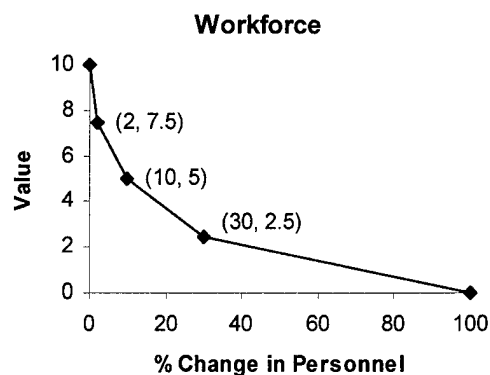
Figure A- 53: VF for Additional Personnel

Additional Workload

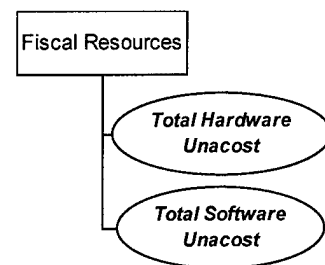   *Additional Workload* evaluates the average number of weekly overtime hours per individual that is required, on average, during the useful life of the countermeasure (or the total incurred due to strategy implementation). This measure is assumed to range from zero to a maximum of 20 overtime-hours per week, where this amount is averaged only over the current and applicable number of employees. Based upon the additional assumption that each person already works 40 hours a week, anything more than 20 overtime-hours (60 hours total) a week (per individual) would be operationally unacceptable. It is assumed that strategies exceeding this limit will either be disregarded or additional personnel would have to be acquired. A notional evaluation function is shown in Figure A- 54.

Additional Workload
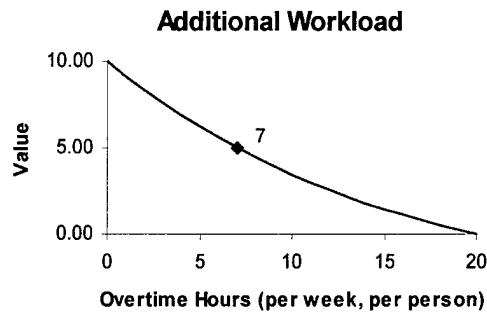
Figure A- 54: VF for Additional Workload

Fiscal Resources

There are several ways that costs of alternatives may be compared, to include the percentage of a given budget or total costs discounted over a specified time period (e.g. net present value). However, each method has several issues to overcome. Using percentages of budgets must accommodate for the different types of budgets, their restrictions, and variation over time. Net present value offers the advantage of discounting money over time, but accounting for strategies with varying lengths of time can be cumbersome (e.g. using the least common multiple of time). [Humphreys, 1991:33] For these reasons, another approach was pursued—discounted uniform annual costs.

Uniform annual cost (Unacost) is the alternative chosen to score IA strategies. The Unacost measure ensures that an equitable comparison between the long-term monetary impact of IA strategies. Unlike using a simple NPV calculation, this method accounts for variations in useful life, and puts "all systems (IA Strategies) on a 1-year basis. Unacost converts any system lasting n years with a present value P_n to an equivalent 1-year cost as of the end of the year" and is denoted by

$$R = P_n F_{PR,i,n} \quad \text{[Humphreys, 1991:35]}$$

Equation A - 1: Unacost

$F_{PR,i,n}$ is the *capital-recovery factor*, which "converts a single zero-time cost to an

equivalent uniform end of year annual cost, *Unacost*." [Humphreys, 1991:27] This factor

requires the inputs interest rate (i) and time period (n) and is determined by the equation

$$F_{PR,i,n} = \frac{i(1+1)^n}{(1+i)^n - 1} \quad \text{[Humphreys, 1991:27]}$$

Equation A - 2: Unacost Factor

For IA Strategy evaluation, the expected useful lives of the components are used as the

duration and an organizationally accepted interest rate is used. Humphreys also notes "Unacosts

can be added together." [1991:38] Therefore, to get an overall Unacost for an IA Strategy, the

Unacost for each element must be calculated and added to all other Unacost figures for that

strategy. An example of this process is shown in the decision support tool *MIA-Hamill.xls*. If

the interest rate chosen is questioned, this method should lend itself to sensitivity analysis.

The fiscal costs were broken down into the two categories (hardware and software) to

capture preferences for each type. It is assumed that funds are available, and will be procured

from the appropriate budget (types of money). Additionally, any alternative considered is

assumed to be within budgetary constraints throughout its life span. Note that the Unacost score

is only a means to facilitate equitable comparisons between strategies and may not be the exact

cost incurred on an annual basis.

Total Hardware Unacosts

Hardware Costs include the dollar costs associated with initial procurement as well as

operations and maintenance (O&M) dollar costs. To implement this measure, each hardware

element proposed in the IA Strategy is evaluated by adding the initial (immediate) cost to the net present value (NPV) of any subsequent costs incurred due to O&M and training. This combined cost of each element is then converted to the Unacost value discussed earlier.

The assumptions for this measure are that the hardware and software elements will have no salvage value, and alternatives that exceed the organization's budget will not be considered. The evaluation measure scale will range between the minimum and maximum Unacosts of alternatives considered, to include doing nothing. If salvage costs are known, they, of course, could be added to the calculations. The max could also be an organizational budgetary limit if capital rationing is present.
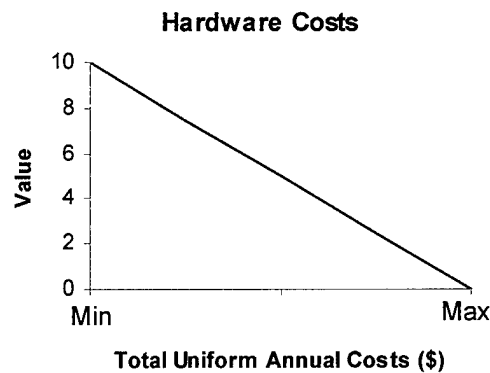
Hardware Costs
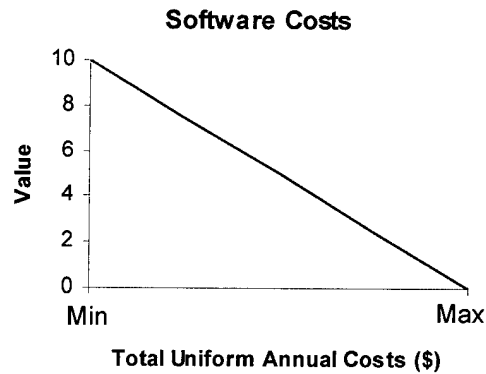

Figure A- 55: VF for Hardware Costs

A further benefit of this type of analysis is that it enables direct comparison of individual components in addition to the overall dollar cost of an entire strategy.

Total Software Unacosts

Software costs will include considerations identical to that of hardware. The total Unacost will include procurement, update and associated training costs.

Software Costs

Figure A- 56: VF for Software Costs

As seen in the hardware costs, the maximum Unacost would be established before the evaluation of alternatives, and may be based upon budgetary limits with an organizationally accepted time period and interest rates as inputs to the process.

Weighting

Once the ranges, shapes and relative level of values are incorporated evaluation functions, the DM must then evaluate the tradeoffs between each of the attributes. The process to accomplish this and the restrictions placed upon them are discussed in Chapter 2.

Summary

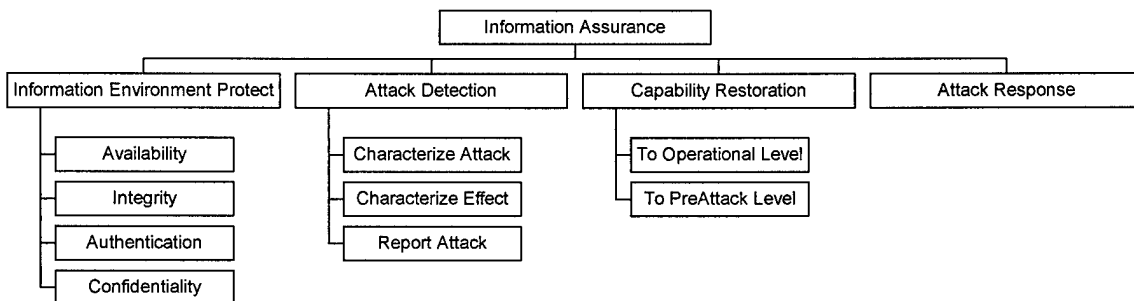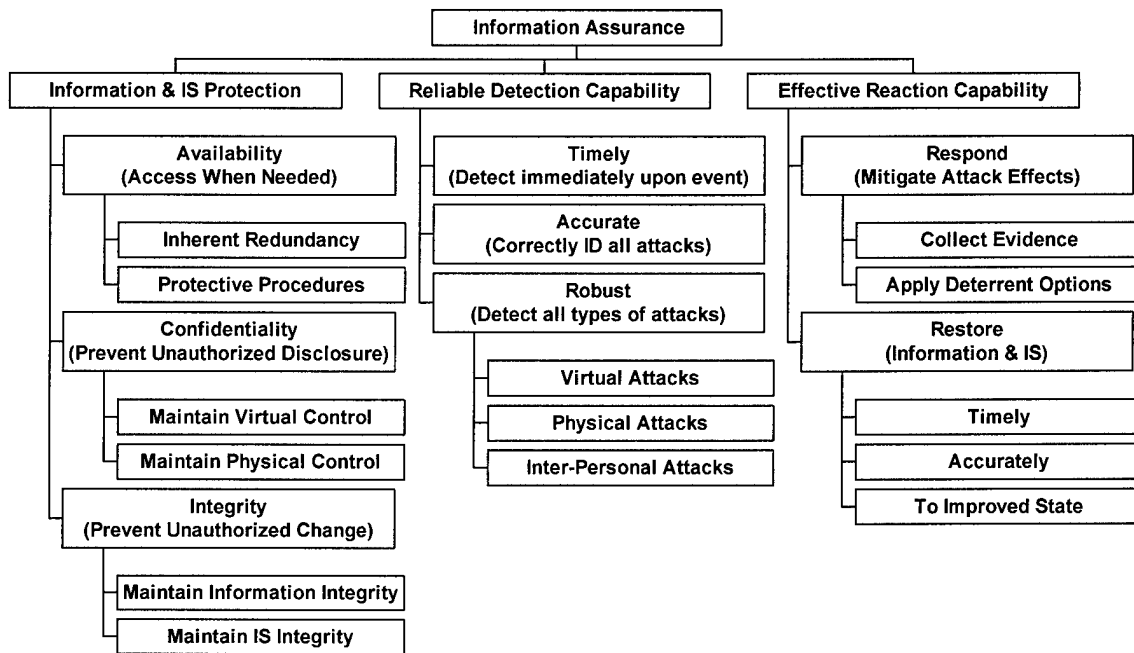Direct and exact measurement of all benefits and costs of IA strategies may remain elusive. However, evaluation of alternatives through comparisons of how they perform with respect to decision maker preferences (taken primarily from doctrine) should facilitate the identification of new alternatives, leading to a cost-effective strategy that enhances functionality and provides the level of Information Assurance required.
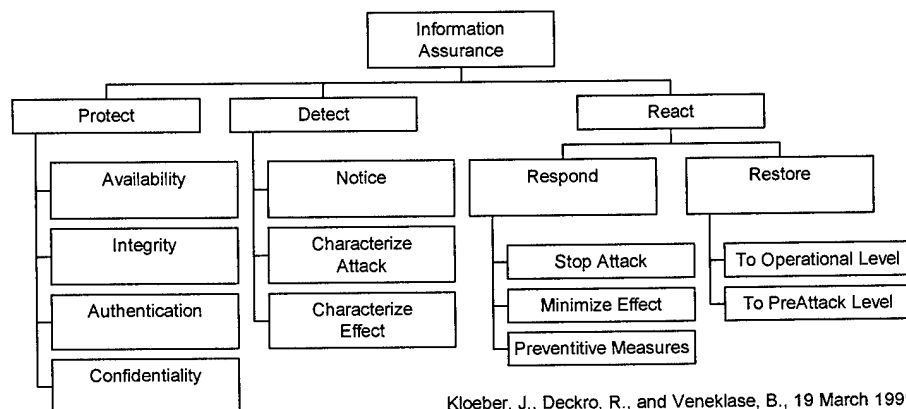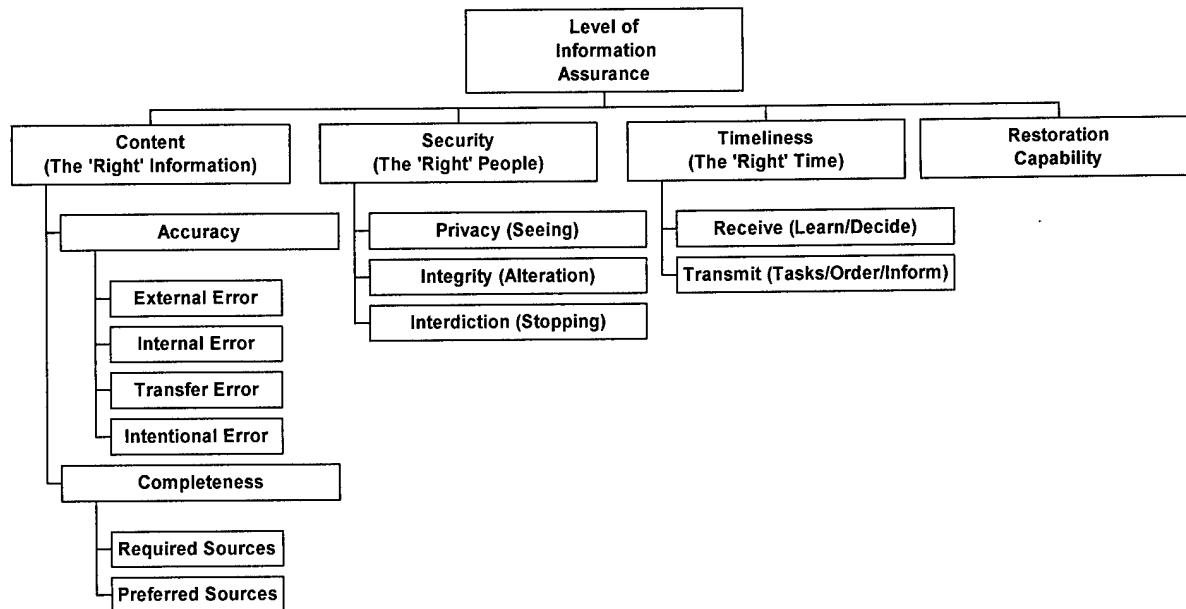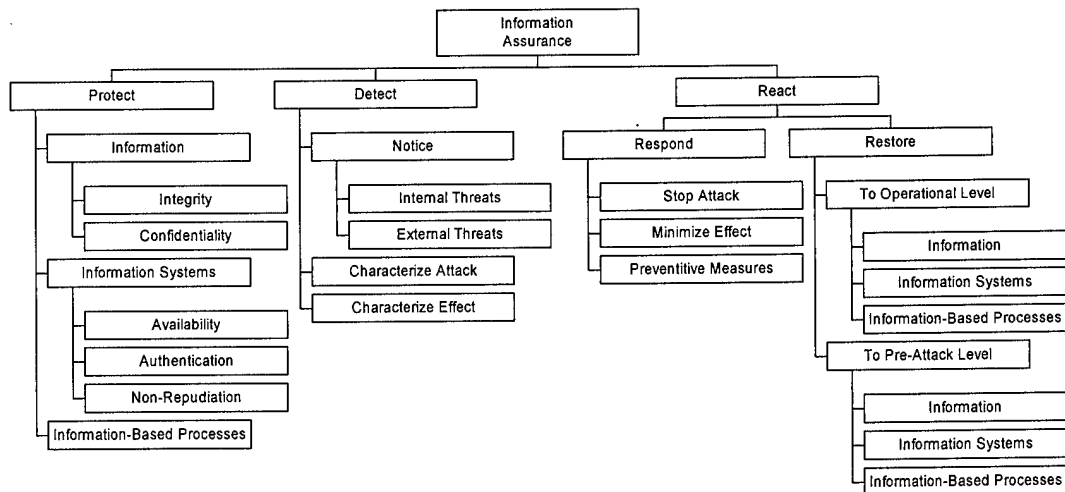
Appendix B – Alternative Hierarchies

Overview

This appendix presents alternative hierarchies that were developed during this research. Each has its merits and shortcomings, but may provide insight towards the development of an improved value model for Information Assurance.

```
                              Information Assurance

  Information & IS Protection    Reliable Detection Capability    Effective Reaction Capability

      Availability                      Timely                         Respond
   (Access When Needed)      (Detect immediately upon event)     (Mitigate Attack Effects)

    Inherent Redundancy             Accurate                       Collect Evidence
                               (Correctly ID all attacks)
    Protective Procedures                                        Apply Deterrent Options
                                       Robust
      Confidentiality          (Detect all types of attacks)           Restore
 (Prevent Unauthorized Disclosure)                              (Information & IS)
                                   Virtual Attacks
    Maintain Virtual Control                                            Timely
                                  Physical Attacks
    Maintain Physical Control                                         Accurately
                                Inter-Personal Attacks
        Integrity                                                 To Improved State
 (Prevent Unauthorized Change)

  Maintain Information Integrity

      Maintain IS Integrity
```

```
                              Information Assurance

 Information Environment Protect   Attack Detection   Capability Restoration   Attack Response

      Availability             Characterize Attack    To Operational Level
       Integrity               Characterize Effect     To PreAttack Level
     Authentication               Report Attack
    Confidentiality
```

B-1

Information Assurance

- Protect
  - Information
    - Integrity
    - Confidentiality
  - Information Systems
    - Availability
    - Authentication
    - Non-Repudiation
  - Information-Based Processes
- Detect
  - Notice
    - Internal Threats
    - External Threats
  - Characterize Attack
  - Characterize Effect
- React
  - Respond
    - Stop Attack
    - Minimize Effect
    - Preventitive Measures
  - Restore
    - To Operational Level
      - Information
      - Information Systems
      - Information-Based Processes
    - To Pre-Attack Level
      - Information
      - Information Systems
      - Information-Based Processes

Level of Information Assurance

- Content (The 'Right' Information)
  - Accuracy
    - External Error
    - Internal Error
    - Transfer Error
    - Intentional Error
  - Completeness
    - Required Sources
    - Preferred Sources
- Security (The 'Right' People)
  - Privacy (Seeing)
  - Integrity (Alteration)
  - Interdiction (Stopping)
- Timeliness (The 'Right' Time)
  - Receive (Learn/Decide)
  - Transmit (Tasks/Order/Inform)
- Restoration Capability

Information Assurance

- Protect
  - Availability
  - Integrity
  - Authentication
  - Confidentiality
- Detect
  - Notice
  - Characterize Attack
  - Characterize Effect
- React
  - Respond
    - Stop Attack
    - Minimize Effect
    - Preventitive Measures
  - Restore
    - To Operational Level
    - To PreAttack Level

Kloeber, J., Deckro, R., and Veneklase, B., 19 March 1999

B-2

Bibliography

Abate, M. L., Diegert, K. V., and H. W. Allen. "A Hierarchical Approach to Improving Data Quality." *Data Quality*, Vol. 4, No 1. 1998, Available at http://www.dataquality.com/998abate.htm.

Alberts, David S. *Defensive Information Warfare.* National Defense University, Institute for National Strategic Studies, The Center for Advanced Concepts and Technology. Washington: GPO, August 1996.

Anderson, R. H., Feldman, P. M., Gerwehr, S., Houghton, B., Mesic, R., Pinder, J. D., Rothenberg, J., and James Chiesa. *Securing the U.S. Defense Information Infrastructure: A Proposed Approach.* Santa Monica: RAND, 1999 (MR-993-OSD/NSA/DARPA).

Andrews, D. *Report of the Defense Science Board Task Force on Information Warfare-Defense (IW-D).* Washington: Office of the Under Secretary of Defense for Acquisition & Technology (OUSDA&T), November 1996.

Boyd, John R. *A Discourse on Winning and Losing.* Unpublished manuscript. Maxwell AFB, AL. Air University Press, 1982.

Buchan, Glenn. "Information War and the Air Force: Wave of the Future? Current Fad?" *RAND Project Air Force Issue Paper.* Santa Monica: RAND, March 1996. Excerpt from published article, http://www.rand.org/publications/IP/IP149.

Chairman of the Joint Chiefs of Staff (CJCS). "Joint Vision 2010," *Joint Force Quarterly*: 35-49 (Summer 1996).

Clemins, A. R. "Information Superiority in the Pacific Fleet." *Joint Force Quarterly*: 67-70 (Autumn/Winter 1997-98).

Computer Emergency Response Team/Coordination Center (CERT/CC). *CERT/CC Statistics: 1988 – 1999.* Pittsburgh: Carnegie Mellon Software Engineering Institute, 20 January 2000. Excerpt from published report, http://www.cert.org/stats/cert_stat.html.

CERT/CC. *Denial of Service.* Pittsburgh: Carnegie Mellon University, Software Engineering Institute, 12 February 1999. n. pag. Excerpt from published report, http://www.cert.org/tech_tips/denial_of_service.html.

Defense Information Systems Agency (DISA). *Information Assurance for Auditors & Evaluators.* Version 1.04. CD-ROM. October 1998.

Department of the Air Force. *Cornerstones of Information Warfare.* Washington: HQ USAF, 1995. Available at http://www.infowar.com/mil_c4i/mil_c4ia.html-ssi.

Department of the Air Force. *Air Force Basic Doctrine.* AFDD 1. Washington: HQ USAF, September 1997.

BIB-1

Department of the Air Force. *Computer Security*. AFI 33-202. Washington: HQ USAF, 1 February 1999.

Department of the Air Force. *Information Protection Security Awareness, Training, and Education (SATE) Program*. AFI 33-204. Washington: HQ USAF, 26 April 1999.

Department of the Air Force. *Identification and Authentication*. AFMAN 33-223. Washington: HQ USAF, 1 June 1998.

Department of the Air Force. *Controlled Access Protection (CAP)*. AFMAN 33-229. Washington: HQ USAF, 1 November 1997.

Department of the Air Force. *The Certification and Accreditation (C&A) Process*. AFSSI 5024, Volume 1. Washington: HQ USAF, 1 September 1997.

Department of the Air Force, USAF Scientific Advisory Board (SAB). *New World Vistas: Air and Space Power for the 21st Century, Information Applications Volume*. Washington: USAF Scientific Advisory Board, 1995.

Department of the Army. *Information Operations*. USA FM 100-6. Washington: HQ USA, 27 August 1996. Available at http://www.fas.org/irp/doddir/army/fm100-6/ch1.htm

Department of Defense. *Security Requirements for Automated Information Systems (AISs)*. DODD 5200.28. Washington: Pentagon, 21 March 1988.

Department of Defense. *DOD Information Technology Security Certification and Accreditation Process (DITSCAP)*. DODI 5200.40. Washington: Pentagon, 30 December 1997.

Department of Defense. *DITSCAP Application Document*. DOD 5200.40-M (Draft). Washington: Pentagon, 21 April 1999.

Department of Defense, Information Assurance Technology Analysis Center (IATAC). 1998a. *Vulnerability Analysis*. Washington: Defense Technical Information Center (DTIC), Spring 1998.

Department of Defense, IATAC. 1998b. *Firewalls*. Washington: DTIC, Fall 1998.

Department of Defense, Joint Chiefs of Staff. *Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms*. Washington: Pentagon, amended through 29 June 1999.

Department of Defense, Joint Chiefs of Staff. *Joint Publication 3-13, Joint doctrine for Information Operations*. Washington: Pentagon, 9 Oct 1998.

Department of Defense, Joint Chiefs of Staff. *Joint Publication 3-13.1, Joint doctrine for Command and Control Warfare (C2W)*. Washington: Pentagon, 7 February 1996.

Department of Defense, Joint Chiefs of Staff. *Information Assurance: Legal, Regulatory, Policy and Organizational Legal, Regulatory, Policy and Organizational Considerations.* (Fourth Edition). Washington: Pentagon, August 1999.

Doyle, M. P. *A Value-Focused Thinking Approach to Offensive Information Operations.* MS thesis, AFIT/GOR/ENS/98M-10. School of Engineering, Air Force Institute of Technology (AU), Wright-Patterson AFB OH, March 1998.

Doyle, M. P., Deckro, R. F., Jackson, J. A., and J. M. Kloeber. *A Value Function Approach to Information Operations MOE's: A Preliminary Study.* Air Force Institute of Technology Center for Modeling Simulation and Analysis: CMSATR 97-04, July 1997.

Doyle, M. P., Deckro, R. F., Kloeber, J. M., and J. A. Jackson. "Measures of Merit for Offensive Information Operations Courses of Action." *Military Operations Research*, forthcoming, 2000.

Ferdman, M. and P. J. DeNyse. *AFIWC Computer Security Engineering Assessments: Process Description and Recommended Enhancements.* (Final Draft) Bedford: MITRE, January 2000.

Fuller, J. F. C. *The Conduct of War: 1789-1961.* New York: Da Capo Press, 1992.

Gertz, B. "Eligible Receiver." *The Washington Times.* April 16, 1998.

Gumahad, A. T., II. "The Profession of Arms in the Information Age." *Joint Force Quarterly*:14-20 (Spring 1997).

Humphreys, K. K. *Jelen's Cost and Optimization Engineering.* (Third Edition). New York: McGraw-Hill, Inc., 1983.

Information Operations Symposium: *Key Technologies for Information Assurance.* 26-28 October 1999. San Diego, CA.

Keeney, R. L. and H. Raiffa. *Decisions with Multiple Objectives: Preferences and Value Tradeoffs.* Cambridge: Cambridge University Press, 1993.

Keeney, R. L. "Creativity in Decision Making with Value-Focused Thinking." *Sloan Management Review*: 33-41 (Summer 1994).

Keeney, R. L., "Using Values in Operations Research." *Operations Research*: 793-813 (September-October 1994).

Keeney, R. L. *Value Focused Thinking: A Path to Creative Decisionmaking.* Cambridge: Harvard University Press, 1998.

Kelso, T. S. 1999a. Vice Commandant, Air Force Institute of Technology, Wright-Patterson AFB OH. Personal interview. 23 November 1999.

Kelso, T. S. 1999b. Vice Commandant, Air Force Institute of Technology, Wright-Patterson AFB OH. Personal interview. 6 December 1999.

Kendall, K. *A Database of Computer Attacks for the Evaluation of Intrusion Detection Systems.* MS thesis. Massachusetts Institute of Technology, June 1999.

Kirkwood, C. W., *Strategic Decision Making: Multiobjective Decision Analysis with Spreadsheets.* Belmont: Duxbury Press, 1997.

Lapin, L. L. *Probability and Statistics for Modern Engineering.* (Second Edition). Belmont: Duxbury Press, 1990.

Large Scale Networking Next Generation Internet Implementation Team. Next Generation Internet: Implementation Plan. February 1998.

Lesser, I. O., Hoffman, B., Arquilla, J., Ronfeldt, D., Zanini, M. *Countering the New Terrorism.* Santa Monica: RAND, 1999 (RAND-MR-989-AF).

Longstaff, T. A., Ellis, J. T., Hernan, S. V., Lipson, H. F., McMillan, R. D., Pesante, L. H., and D. Simmel. *Security of the Internet.* Pittsburgh: Carnegie Mellon University, Software Engineering Institute, 1997. n. pag. Excerpt from published article, http://www.cert.org/encyc_article/tocencyc.html

Materna, R. D. *Assessing the Value of Information Technology.* Dayton: Strategic Consulting Group, NCR, March 1992.

Maynard, L. W. 1999a. Chief, Systems Administration Branch, Air Force Institute of Technology, Wright-Patterson AFB OH. Personal interview. 8 November 1999.

Maynard, L. W. 1999b. Chief, Systems Administration Branch, Air Force Institute of Technology, Wright-Patterson AFB OH. Personal interview. 24 November 1999.

Maynard, L. W. Chief, Systems Administration Branch, Air Force Institute of Technology, Wright-Patterson AFB OH. Personal interview. 11 January 2000.

MITRE. *Defense—Information Assurance Red Team Methodology.* Bedford: Center for Integrated Intelligence Systems, May 1999. (For Official Use Only)

Molander, R.C., Wilson, P. A., Mussington, D. A., Mesic, R. F. *Strategic Information Warfare Rising.* Santa Monica: RAND, August 1999 (MR-964-OSD). Available at http://www.rand.org/publications/MR/MR964/index.html.

Monks, J. G. *Operations Management: Theory and Problems.* New York: McGraw-Hill, 1977.

Murty, K. G. *Operations Research: Deterministic Optimization Models.* Englewood Cliffs: Prentice Hall, 1995.

National Computer Security Center (NCSC). *Accreditor's Guideline.* NCSC-TG-032, Version 1. 6 March 1997.

National Security Telecommunications and Information Systems Security Committee (NSTISSI). *National Information Systems Security (INFOSEC) Glossary (Revision 1).* NSTISSI No. 4009. Fort Meade: National Security Agency, January 1999.

President's Commission on Critical Infrastructure Protection (PCCIP). *Critical Foundations: Thinking Differently.* Washington: GPO, October 1997. Available at http://www.infowar.com.

President, Executive Order. "Classified National Security Information, Executive Order 12958." *Federal Register* 60, no. 76 (20 April 1995).

Ware, W. H. *The Cyber-Posture of the National Information Infrastructure.* Santa Monica: RAND, 1998 (RAND MR-976-OSTP).

Whitehead, P. *Teach Yourself Networking Visually.* Foster City: IDG Books Worldwide, 1997.

VITA

Captain J. Todd Hamill was born on 2 September 1969 in Alabama. Upon graduation from Southside High School in Fort Smith, Arkansas, he enlisted in the United States Air Force as a medical administrative specialist. After just over one year of active duty service, he was accepted to the United States Air Force Academy Preparatory School, and eventually graduated from the United States Air Force Academy in June of 1993. His first assignment was as an analyst supporting precision guided munitions evaluations. During his second tour as a B-2 survivability analyst, he completed a Master of Science Degree in Industrial Engineering at New Mexico State University. Finally, his third assignment brought Captain Hamill to AFIT as a degree candidate. From AFIT, Captain Hamill reports to Space and Missile Systems Center as a scientific analyst.

ABSTRACT (Maximum 200 Words)

The information revolution has brought forth new and improved capabilities to rapidly disseminate and employ information in decision-making. These capabilities are critical to the civilian and military infrastructures of the United States, and act as force enhancers and enablers for the Armed Forces. These capabilities, however, often rely upon systems interconnected throughout the world, resulting in potentially increased vulnerability to attack. To add to this problem, elusive, threatening forces (national and transnational) originating from anywhere on the globe are likely to offer opponents less reliant on information technology an asymmetric advantage over information-reliant nations like the United States.

To date, effective methods and measures to specifically value information and information systems are lacking. This thesis develops a first cut methodology facilitating the identification of key information, generating information assurance strategies and implementing measures to assess them.